NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SPECIAL OPERATIONS AND CYBER WARFARE

by

Jason C. Tebedo

December 2016

Thesis Advisor:	Dorothy Denning
Second Reader:	Duane Davis

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
SPECIAL OPERATIONS AND CYBER WARFARE

5. FUNDING NUMBERS

6. AUTHOR(S) Jason C. Tebedo

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

As the United States Special Operations Command (USSOCOM) prepares for future conflicts, some have questioned its ability to conduct Special Warfare and Surgical Strike in all domains of warfare, to include the cyber domain. This thesis examines the applicability of cyber operations to U.S. special operations and whether the cyber support provided by the United States Cyber Command (USCYBERCOM) is sufficient to meet USSOCOM's potential cyber requirements. It explores USSOCOM's congressionally mandated core activities and how cyber operations could promote such activities. Finally, the thesis provides a decision theory and operational design analysis of how USSOCOM could build its own internal cyber capability - if USSOCOM determines USCYBERCOM cannot meet the cyber requirements of the special operations community.

The researcher was unable to conclude as to whether USCYBERCOM's cyber support to USSOCOM was sufficient. USCYBERCOM's cyber support structure is still too immature for analysis and therefore necessitates future research by USSOCOM. The thesis does conclude USSOCOM can improve their special operation's efficacy by incorporating the cyber domain. Finally, the research concludes, if USSOCOM were to build a cyber capacity, the reflagging of the 95th Civil Affairs Brigade would be the best course of action.

14. SUBJECT TERMS
cyber domain, cyber warfare, special operations, core activities, Special Warfare, Surgical Strike, future warfare, technology, low intensity conflict, Internet, networks, non-state actors, state actors, Russia, China, Ukraine, cyber command, Duggan, direct action, unconventional warfare

15. NUMBER OF PAGES
77

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

SPECIAL OPERATIONS AND CYBER WARFARE

Jason C. Tebedo
Major, United States Army
B.S., Western Michigan University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2016

Approved by: Dr. Dorothy Denning
Thesis Advisor

Dr. Duane Davis
Second Reader

Dr. John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the United States Special Operations Command (USSOCOM) prepares for future conflicts, some have questioned its ability to conduct Special Warfare and Surgical Strike in all domains of warfare, to include the cyber domain. This thesis examines the applicability of cyber operations to U.S. special operations and whether the cyber support provided by the United States Cyber Command (USCYBERCOM) is sufficient to meet USSOCOM's potential cyber requirements. It explores USSOCOM's congressionally mandated core activities and how cyber operations could promote such activities. Finally, the thesis provides a decision theory and operational design analysis of how USSOCOM could build its own internal cyber capability - if USSOCOM determines USCYBERCOM cannot meet the cyber requirements of the special operations community.

The researcher was unable to conclude as to whether USCYBERCOM's cyber support to USSOCOM was sufficient. USCYBERCOM's cyber support structure is still too immature for analysis and therefore necessitates future research by USSOCOM. The thesis does conclude USSOCOM can improve their special operation's efficacy by incorporating the cyber domain. Finally, the research concludes, if USSOCOM were to build a cyber capacity, the reflagging of the 95th Civil Affairs Brigade would be the best course of action.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADCON	Administrative Control
AFSOC	Air Force Special Operations Command
BPC	Building Partner Capacity
CA	Civil Affairs
CAO	Civil Affairs Operations
CAS	Close Air Support
CMF	Combat Mission Forces
COIN	Counterinsurgency
CPF	Cyber Protection Forces
CT	Counterterrorism
CWMD	Countering Weapons of Mass Destruction
DA	Direct Action
DOD	Department of Defense
DODIN	Department of Defense Information Network
FHA	Foreign Humanitarian Aid/Assistance
FID	Foreign Internal Defense
FOC	Full Operational Capability
GCC	Geographic Combatant Commands
HRR	Hostage Rescue and Recovery
HRR	Hostage Rescue and Recovery
IO	Information Operations
ISIS	Islamic State
JCET	Joint Capability Exchange Training
JCSOC	Joint Cyber Special Operations Command
JIIM	Joint, Interagency, Intergovernmental, and Multinational
JOPP	Joint Operating/Operational Planning Process
JP	Joint Publication
JSOC	Joint Special Operations Command
MARSOC	Marine Special Operations Command

MFP	Major Force Program
MISO	Military Information Support Operations
MLE	Military Liaison Elements
NAVSPECWARCOM	Naval Special Warfare Command
NGO	Non-governmental organizations
NMF	National Mission Forces
NSA	National Security Agency
OPCON	Operational Control
OPE	Operational Preparation of the Environment
OSD	Office of the Secretary of Defense
POTUS	President of the United States
PSYOP	Psychological Operations
SCADA	Supervisory Control and Data Acquisition
SecDef	Secretary of Defense
SFA	Security Force Assistance
SOAR	Special Operations Aviation Regiment
SOF	Special Operations Forces
SR	Special Reconnaissance
STRATCOM	United States Strategic Command
TACON	Tactical Control
TMA	Traditional Military Activities
TSOC	Theater Special Operations Commands
USACAPOC	United States Army Civil Affairs and Psychological Operations Command
USASOC	United States Army Special Operations Command
USCYBERCOM	United States Cyber Command
USG	U.S. Government
USSOCOM	United States Special Operations Command
UW	Unconventional Warfare
VEO	Violent Extremist Organization
WMD	Weapons of Mass Destruction

ACKNOWLEDGMENTS

This thesis couldn’t be possible without the generosity and willingness of kind individuals. My sincerest thanks are extended to all of those who helped along this long process. Firstly, I would like to give thanks to my Lord and Savior, Jesus Christ. His wisdom gave me the strength, perseverance, and forethought required to finish this thesis. God has given me inspiration and guidance all throughout this extensive process.

I would also like to express my sincerest thanks to my friends and family, all of whom were instrumental in my completing this assignment. In particular, I wish to thank my daughter, Alexis Tebedo, for reminding me that life is fun and not to be taken too seriously, and for always supporting me even though we are worlds apart.

I am highly indebted to and am humbled by my thesis advisor, Dr. Dorothy Denning, for the inspiration and motivation, and for keeping me disciplined throughout this endeavor. To Dr. Arquilla, I cannot say enough for your professionalism and dedication to the special operations community. You truly are an example for others to follow. Finally, Dr. Davis, thank you for inspiring me to pursue the cyber domain. Your enthusiasm for cyber operations is contagious.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Special Operations Forces (SOF) generally are described as close-knit, specifically structured units staffed through a judicious screening and selection process for missions that either require a high degree of technical expertise or are politically sensitive in nature. SOF uses adaptive tools and accomplishes the goals and objectives of the nation through the use of irregular warfare and the employment of unconventional tactics against strategic and operational objectives. The modern battlefield juxtaposed with the United States Special Operations Command's (USSOCOM) intent to synchronize the SOF Operations and provide SOF to Geographic Combatant Commands (GCC), generates an interesting question. If USSOCOM is charged with providing SOF support to the GCCs but is unable to provide adequate unconventional/irregular effects in all domains of warfare (specifically in the cyber domain), does it still fulfill its assigned charter to the GCCs.

A. RESEARCH QUESTION(S)

1. Main Question

This thesis centers on examining the overall question: is USSOCOM's posture for cyber operations effective for the current and future operating environment?

2. Sub-question One

Following the debate surrounding USSOCOM's application of the cyber domain and counterterrorism activities, the researcher will analyze USSOCOM's missions, Surgical Strike and Special Warfare. The mission analysis will be conducted to address an operational query as to whether core elements of USSOCOM's counterterrorism operations are sufficient as is or whether there is room for improvement through the incorporation of cyber operations.

3. Sub-question Two

As currently designed, USSOCOM does not have its own cyber organization and instead relies on cyber support from USCYBERCOM. USCYBERCOM provides cyber support teams to augment USSOCOM's Special Operations Forces (SOF) global mission requirements. The question explored here is whether this arrangement meets USSOCOM's requirement or if USSOCOM needs its own internal cyber force. If the latter, how could USSOCOM build such a unit?

B. PURPOSE AND SCOPE

1. Purpose

Defining purpose within the research, the research is designed to address how USSOCOM can best incorporate cyberwarfare into its operations.

2. Rationale for Study

The rationale for the study is that cyberspace is a warfighting domain that USSOCOM needs to operate in effectively along with the other domains. Unlike similar domains, like the Air and Space Domains, the Cyber Domain is not as easily incorporated into USSOCOM's unique mission set. USSOCOM's incorporation of cyber effects, as discussed below, requires immense coordination, confidentiality, and extreme attention to detail—all of which are difficult to achieve from an outside perspective

Cyber operations enhance traditional military activities and are becoming a critical engagement strategy for state and non-state actors. The evolution of traditional military activities creates a question with regard to USSOCOM's approach to modern warfare. Is USSOCOM's current "supported model" sufficient or does it need its own internal cyber unit? Current cyber support operations draw parallels to the inter-organizational Close Air Support (CAS) provided to special operations forces in the early stages of the Iraq and Afghanistan conflicts. In contrast, an internal cyber component may best fit the unit's operational needs as did the need to create a SOF specific (internal) aviation regiment 160th Special Operations Aviation Regiment (SOAR).

C. METHODOLOGY

The researcher will utilize an empirical-analytical approach that draws on existing literature, operational art, and decision theory. The research examines current and historic literature pertaining to the mission, doctrine, organization, manpower, and resources of USCYBERCOM and USSOCOM. Specifically, the literature referenced will be used to analyze existing SOF and cyber theory that concerns the unique mission of USSOCOM and the current cyber support structure provided by USCYBERCOM. Current literature surrounding Special Operation’s missions and operational requirements will be examined for the purpose of analyzing whether USCYBERCOM can meet USSOCOM’s mission requirements or whether USSOCOM needs its own cyber component. Although the result of this analysis is inconclusive, the thesis will apply operational art, specifically operational design, to determine how best to organize an internal cyber capability within USSOCOM, should that strategy be deemed preferable at some time in the future. For the purpose of identifying the most effective strategy for a potential cyber component within USSOCOM, the researcher will utilize quantifiable decision theory. Specific focus is placed on where the cyber billets would come from, in particular, whether they would be new authorizations or acquired by reflagging an existing unit of USSOCOM.

D. THESIS STRUCTURE

Chapter II examines mission and core capabilities of USSOCOM to determine the role of cyber operations in USSOCOM. Chapter III examines the current state of USCYBERCOM, and how it supports USSOCOM. It then identifies and analyzes nine criteria for assessing whether USSCOCOM’s cyber operations are best served by the current arrangement where cyber forces are supplied by USCYBERCOM or by USSOCOM building its own cyber component. Finally, Chapter IV applies operational art and decision theory to determine the best approach for building a cyber capability within USSOCOM if that strategy is pursued.

THIS PAGE INTENTIONALLY LEFT BLANK

II. APPLICATION OF CYBER OPERATIONS TO USSOCOM'S MISSION

The private, public and commercial sector are now subject to a new world order whereas the dangers of online operations are now more progressively complex. In response to this complex threat, the Department of Defense's (DOD) Unified Campaign Plan (UCP) assigned "USSOCOM the responsibility for synchronizing DOD plans against global terrorist networks and, as directed, conducting global operations against those networks."[1] USSOCOM is chartered under Title 10 to operate as a "global SOF provider with the inherent responsibility to coordinate global SOF operations with the Services, Combatant Commanders, the Joint Staff, and the Office of the Secretary of Defense (OSD)."[2]

Taking a step back and analyzing USSOCOM, few would take the position that USSOCOM's operators are untrained, ill equipped, and unprepared to fight terrorist networks. However, the operational planning and execution against terrorist networks requires the incorporation of all domains of warfare, especially the cyber domain. A debate remains as to whether USSOCOM is prepared to address cyber special operations as part of worldwide counterterrorism requirements.

A. SPECIAL OPERATIONS AND CYBER

Although the formal integration of cyber operations into special operations is currently debated among scholars, politicians, and military leaders (as described in subsequent writings), the 21st century revolution in cyber warfare necessitates that the United States Government (USG) conduct further review of the applicability of full cyber SOF integration. As a reference to the global cyber/defense revolution, other nations have

[1] Andrew Feickert, U.S. Special Operations Forces (SOF): Background and Issues for Congress (CRS Report No. RS21048) (Washington, DC: Congressional Research Service, 2016), 2, https://fas.org/sgp/crs/natsec/RS21048.pdf

[2] Ibid., 7.

already combined special operations and cyber warfare with overwhelmingly positive effects.[3] Elite special operations units from Iran's Revolutionary Guard, known as Quds Force," reportedly used similar tactics online to identify and take out ringleaders of the failed "Green Revolution to overthrow then-Iranian President Mahmoud Ahmadinejad in 2009."[4] Though early in the concept of cyber warfare and special operations, Iran was progressive in thinking when they later integrated a civilian cyber force—a part of Quds Force units. This hybrid SOF/civilian cyber force was utilized under the same cyber warfare methodology when addressing insurgent opposition leaders fighting to overthrow Syrian President Bashar Assad.[5]

In the Eastern Theater, Russian SOF outsourced the help from civilian cyber actors and criminal cyber organizations to conduct operations in the Ukraine and Crimea. The combination of cyber and SOF allowed Moscow the opportunity to gain territory (Crimea) without ever conducting phase three operations.[6] The examples incorporating cyber operations into hybrid/irregular warfare tactics by Iran and Russia provided above outline a potential road for other U.S. adversaries to follow.[7]

B. USSOCOM'S REQUIREMENTS

As an overview of USSOCOM and its congressionally mandated mission, USSOCOM defines its mission along two macro and twelve micro operational lines. The two lines defined at the macro level are Surgical Strike and Special Warfare, while the twelve at the micro level are defined as core activities. These lines of effort allow the

[3]Carlo Munoz, "Do Special Operations Forces Need Their Own Elite Cyberwarfare Team?" *The Daily Dot*. January 19, 2016. Accessed May 05, 2016. http://www.dailydot.com/opinion/special-operations-elite-cyberwarfare-team/; Patrick Duggan, "Man, Computer, and Special Warfare," *Small Wars Journal* (January 2016), accessed December 14, 2016, http://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare.

[4] Ibid.

[5] Carlo Munoz, "Do Special Operations Forces Need Their Own Elite Cyberwarfare Team*?" The Daily Dot*. January 19, 2016. Accessed May 05, 2016. http://www.dailydot.com/opinion/special-operations-elite-cyberwarfare-team

[6] Ibid.

command to synchronize its operations in support of oversees contingency operations against transnational terrorist organizations while ensuring unity of effort within the command. Without a defined role at the micro and macro levels, USSOCOM would not be able to properly lobby for resources in support of worldwide operations.

1. Special Warfare

Special Warfare is commonly characterized as Unconventional Warfare, Psychological Warfare, and/or Political Warfare. According to the Joint Publication (JP) 3–05, Special Warfare is,

> The execution of activities that involve a combination of lethal and nonlethal actions taken by specially trained and educated forces that have a deep understanding of cultures and foreign language, proficiency in small unit tactics, subversion, sabotage and the ability to build and fight alongside indigenous combat formations in a permissive, uncertain or hostile environment.[8]

Special Warfare operators preserve expertise in specialized low-level maneuvers; they train in conjunction with indigenous proxy organizations in a permissive, inexact, or aggressive environment.[9] Special Warfare operations are coined white SOF because they are typically those missions that are sensitive in nature but are not necessarily what the media would define as high profile or high risk.

2. Surgical Strike

In contrast, black SOF or Surgical Strike, typically involves lethal operations. Surgical Strike is defined in Joint Publication 3–05 as,

> The execution of activities in a precise manner that employ special operations forces in hostile, denied, or politically sensitive environments

[8] U.S. Joint Chiefs of Staff. *Special Operations*. Joint Publication 3-05. Washington, DC: Joint Chiefs of Staff, April 18, 2010.

[9] David S. Maxwell, “Thoughts on the Future of Special Operations” *Small Wars Journal* (October 31, 2013), http://smallwarsjournal.com/jrnl/art/thoughts-on-the-future-of-special-operations.

to seize, destroy, capture, exploit, recover or damage designated targets, or influence threats.[10]

Figure 1, provided by the United States Army Special Operations Command (USASOC), highlights how the micro and macro levels of effort merge to create synergistic effects.

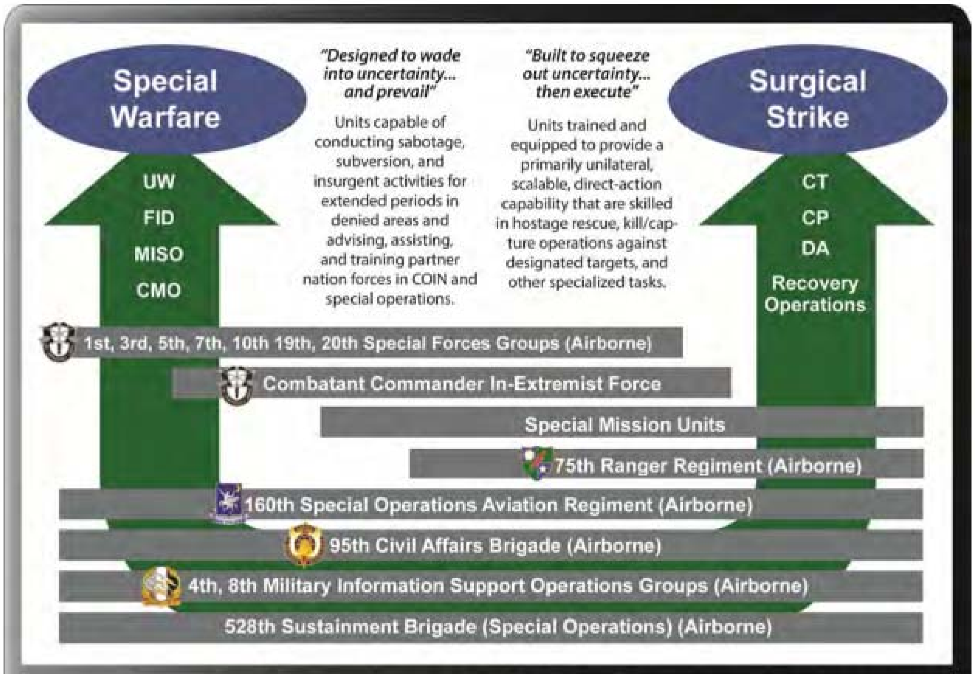

Special Warfare
"Designed to wade into uncertainty... and prevail"
Units capable of conducting sabotage, subversion, and insurgent activities for extended periods in denied areas and advising, assisting, and training partner nation forces in COIN and special operations.
"Built to squeeze out uncertainty... then execute"
Units trained and equipped to provide a primarily unilateral, scalable, direct-action capability that are skilled in hostage rescue, kill/capture operations against designated targets, and other specialized tasks.
Surgical Strike
UW
FID
MISO
CMO
CT
CP
DA
Recovery Operations
1st, 3rd, 5th, 7th, 10th 19th, 20th Special Forces Groups (Airborne)
Combatant Commander In-Extremist Force
Special Mission Units
75th Ranger Regiment (Airborne)
160th Special Operations Aviation Regiment (Airborne)
95th Civil Affairs Brigade (Airborne)
4th, 8th Military Information Support Operations Groups (Airborne)
528th Sustainment Brigade (Special Operations) (Airborne)

Figure 1. Army SOF Surgical Strike and Special Warfare.[11]

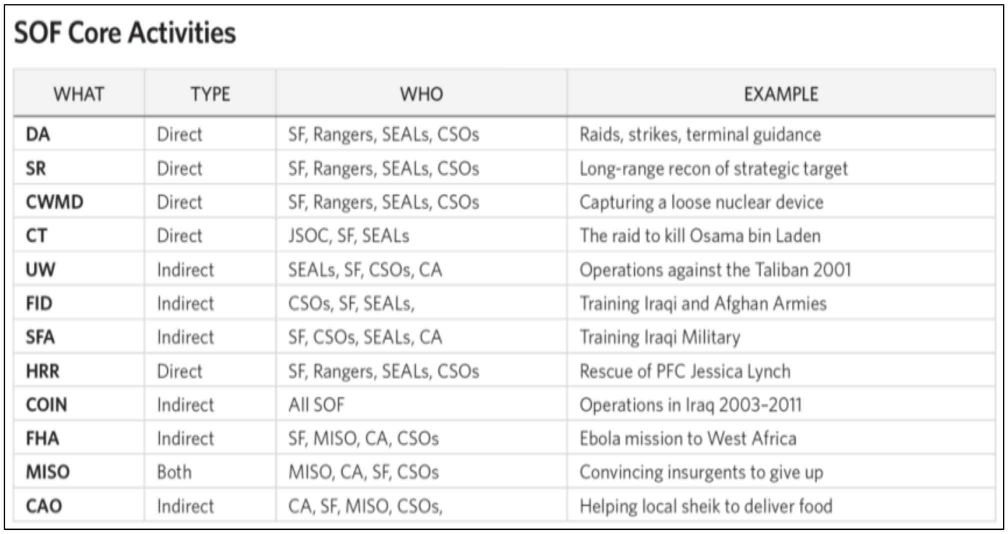
3. USSOCOM's Core Activities

At the micro level, the Department of Defense directs USSOCOM to organize, train, and equip in preparation for Surgical Strike and Special Warfare mission. The Surgical Strike activities (direct) conducted by USSOCOM are Direct Action (DA), Special Reconnaissance (SR), Countering Weapons of Mass Destruction (CWMD), and

[10] U.S. Joint Chiefs of Staff. *Special Operations*, Joint Publication 3-05, Washington, DC: Joint Chiefs of Staff, April 18, 2010.

[11] U.S. Department of the Army, *ARSOF Operating Concept 2022 U.S. Army Special Operations Command*, Washington, DC: U.S. Department of the Army, September 30, 2015.

Counterterrorism (CT), while the Special Warfare activities (indirect) are Unconventional Warfare (UW), Foreign Internal Defense (FID), Security Force Assistance (SFA), Hostage Rescue and Recovery (HRR), Counterinsurgency (COIN), Foreign Humanitarian Aid (FHA), Military Information Support Operations (MISO), and Civil Affairs Operations (CAO).[12] Each core activity is presented within Figure 2. The figured showed which unit is responsible, whether it is an indirect or direct approach, and an example of its application.



SOF Core Activities

WHAT	TYPE	WHO	EXAMPLE
DA	Direct	SF, Rangers, SEALs, CSOs	Raids, strikes, terminal guidance
SR	Direct	SF, Rangers, SEALs, CSOs	Long-range recon of strategic target
CWMD	Direct	SF, Rangers, SEALs, CSOs	Capturing a loose nuclear device
CT	Direct	JSOC, SF, SEALs	The raid to kill Osama bin Laden
UW	Indirect	SEALs, SF, CSOs, CA	Operations against the Taliban 2001
FID	Indirect	CSOs, SF, SEALs,	Training Iraqi and Afghan Armies
SFA	Indirect	SF, CSOs, SEALs, CA	Training Iraqi Military
HRR	Direct	SF, Rangers, SEALs, CSOs	Rescue of PFC Jessica Lynch
COIN	Indirect	All SOF	Operations in Iraq 2003-2011
FHA	Indirect	SF, MISO, CA, CSOs	Ebola mission to West Africa
MISO	Both	MISO, CA, SF, CSOs	Convincing insurgents to give up
CAO	Indirect	CA, SF, MISO, CSOs,	Helping local sheik to deliver food

Figure 2. USSOCOM’s Core Activities.[13]

C. CYBER SURGICAL STRIKE (CORE ACTIVITIES)

1. Direct Action

Joint Publication 3–05 defines the core activity “Direct Action (DA) as, short-duration strikes and other small-scale offensive actions conducted as a special operation

[12] U.S. Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05, Washington, DC: Joint Chiefs of Staff, April 18, 2010.

[13] Steve Bucci, “The Importance of Special Operations Forces Today and Going Forward,” The Heritage Foundation. Accessed May 4, 2016. http://index.heritage.org/military/2015/important-essays-analysis/importance-special-operations-forces-today-going-forward/.

in hostile, denied, or diplomatically sensitive environments and which employ specialized military capabilities to seize, destroy, capture, exploit, recover, or damage designated targets."[14] Aside from the very kinetic engagements in Iraq and Afghanistan, as a whole DA engagements only account for a fraction of total SOF mission load. A possible reason for the public association of SOF and DA is the large media factor associated with these operations. The killing of high profile targets, such as Abu Mus'ab al-Zarqawi and Usama Bin Laden as well as movies and video games are prime instigators of this public perception.

With regard to DA and the cyber domain, Colonel Duggan, cyberwarfare scholar, generally believes the core philosophy supporting all cyber special operations is around the idea of promoting cyber technology's asymmetry to strengthen the rudimentary characteristics of DA missions.[15] If appropriately utilized, cyber knowhow can intensify a DA mission.[16] As with other core activities, cyber warfare in itself is not an effective method of employment. Cyber effects are best used in combination with elements of the other domains.

The big question posed is, of all the United States Government (USG) organizations, which organization is more seasoned to engage in DA missions than SOF who have been conducting this brand of warfare against insurgent groups for the past three decades?[17] Highlighting an ongoing real-world cyber DA mission, the lesser-known Joint Special Operations Command (JSOC) already mentors foreign DA groups in Iraq and Syria and is organizationally responsible for killing members of the Islamic State's (ISIS) cyber caliphate - including Siful Haque Sujan, suspected English-born hacker who

[14] "Joint Publication 3-05, Joint Special Operations." Apr 2011. Council on Foreign Relations. Dec 2016, X.

[15] Patrick Duggan, "Man, Computer, and Special Warfare," *Small Wars Journal* (January 4, 2016), accessed December 14, 2016, http://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare.

[16] Ibid.

[17]Carlo Munoz.,"Do Special Operations Forces Need Their Own Elite Cyberwarfare Team?" *The Daily Dot*. January 19, 2016. Accessed May 05, 2016. http://www.dailydot.com/opinion/special-operations-elite-cyberwarfare-team/.

was recognized as a top Islamic State facilitator of online operations.[18] Though the process of killing or injuring an enemy combatant will nearly always necessitate the use of kinetic weaponry, in the near term future, an attacker may be able to utilize the cyber domain for DA attacks. Employing malware that can cause a computer's battery to explode or quite possibly attacking a vulnerable system such as a Supervisory Control and Data Acquisition (SCADA), as represented through the Aurora Experiment, are potential applications of DA Cyber.[19] Other examples include disabling adversary security systems and alarms, and disabling adversary communications to support a raid.

2. Special Reconnaissance

The core activity Special Reconnaissance (SR) is defined under Joint Publication 3–05 as, "reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or diplomatically and/or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces."[20] To give reference, SR in regards to nation states relates to the communal term espionage. The most common form of the core SR activity in the DOD is Operational Preparation of the Environment (OPE).

Cyber weapons have multiple functions and can be used for espionage or OPE. It is important to highlight the similarities between the intelligence world, espionage, and special operations SR. The domains of cyber-centric SR and traditional intelligence/espionage both involve hacking or breaking into a state's logical/human network and will mostly likely utilize the same methods and technology to do so.[21] Edward Lucas, author of *Cyberphobia: Identity, Trust, Security and the Internet*,

[18] Carlo Munoz, "Do Special Operations Forces Need Their Own Elite Cyberwarfare Team?" *The Daily Dot*. January 19, 2016. Accessed May 05, 2016. http://www.dailydot.com/opinion/special-operations-elite-cyberwarfare-team/.

[19] Scott D Applegate, "The Dawn of Kinetic Cyber," In Cyber Conflict (CyCon), 2013 5th International Conference on, pp. 1–15. IEEE, 2013.

[20] U.S. Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05. Washington, DC: Joint Chiefs of Staff, April 18, 2010.

[21] Edward Lucas, *Cyberphobia: Identity, Trust, Security and the Internet* (London: Bloomsbury Publishing, 2015), Chapter 8.

observes that there is a strong real-life close relationship between the spy domain amid intelligence collection (finding things out) and special operations (direct action). A prime example of this is the killing of Usama Bin Laden. The Central Intelligence Agency (CIA) was responsible for collecting the intelligence, but it was the DOD that conducted the physical operation.

Developing a capacity to conduct cyber SR, and its subordinate OPE, may economize USSOCOM's manpower, resources, and time. Cyber reconnaissance and intelligence gathering is infinitely easier than the routine methods of espionage, as seen during the Cold War.[22] It is difficult to overstate the extreme exertion of resources to recruit a dependable agent and put such an agent into the precise place in an organization so that he or she can duplicate and extract a significant quantity of valued material.[23] The ability to infiltrate an open and unsecure network would cost pennies on the dollar in comparison to the extensive resources involved with human intelligence. Expanding on this point, potential inexpensive applications of cyber SR could include exploiting a terrorist's computer or cell phone to turn on a web-camera and microphone.

Cyber SR may also prove useful for attributing adversary cyber operations. As pointed out in the 2015 Special Operations Manual published by USSOCOM, the advances in cyber technology may allow USSOCOM the ability to uncover cyber attribution, which terrorist networks typically conceal.[24] While malicious cyber actors can penetrate or interrupt targeted cyber networks, most terrorist networks can no longer accept that these cyber undertakings will continue unnoticed.[25] These networks now must assume their personal identities will at some point be revealed. To date, USSOCOM has made noteworthy developments in identifying and attributing cyber infringements.[26]

[22] Richard A Clarke, and Robert K. Knake. *Cyber war*. HarperCollins, 2011, Kindle 3281–3283.

[23] Ibid.

[24] "Special Operations Forces Reference Manual," Federation of American Scientist, June 2015, accessed December 15, 2016, https://fas.org/irp/agency/dod/socom/ref-2015.pdf.

[25] "Special Operations Forces Reference Manual," Federation of American Scientist, June 2015, accessed December 15, 2016, https://fas.org/irp/agency/dod/socom/ref-2015.pdf.

[26] Ibid.

3. Countering Weapons of Mass Destruction

Countering Weapons of Mass Destruction (CWMD) is defined in JP 3–05 as, "USG activities that are conducted to ensure the U.S. and its Armed Forces, allies, partners, and interests are neither coerced nor attacked with WMD."[27] As far as USSOCOM is concerned, the "primary role of SOF for CWMD is preventing WMD development, proliferation, and use."[28] Presidential Decision Directive 39 provides the legal basis for the DOD and, ultimately, USSOCOM to respond to threats of WMD.

In the February 2012 Worldwide Threat Assessment brief to Congress, James Clapper, Director of National Intelligence, emphasized the importance of cyber operations as he identified cyber as the third major hazard facing the U.S., after "terrorism and proliferation of weapons of mass destruction."[29] Everyday cyber capabilities and terrorist networks continue to grow while nuclear powers, such as Russia, Pakistan, and North Korea become weaker. Ruling out the possibility of a terrorist network acquiring nuclear material and utilizing the cyber domain to facilitate operations could be a strategic misstep for the United States and its partners.

STUXNET, a piece of malware designed to destroy nuclear centrifuges in Iran, is a prime example of cyber CWMD operations. The *New York Times* reported that STUXNET was designed "to mess with Iran's best scientific minds" and "make them feel they were stupid."[30] Whether it made them feel stupid or incapable of developing a nuclear weapon, there is no doubt the attack set the program back to the tune of 6 months to 2 years. This interruption, however, provided legislators "both the time and diplomatic

[27] U.S. Joint Chiefs of Staff. *Special Operations*, Joint Publication 3-05, Washington, DC: Joint Chiefs of Staff, April 18, 2010.

[28] Ibid.

[29] James R. Clapper, "Worldwide Threat Assessment to the House Permanent Select Committee on Intelligence," *Statement for the Record, House Permanent Select Committee on Intelligence, 112th Cong., 2nd Sess* (2012): 1.

[30]Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2016), 2.

breathing room to assess Iran's true intentions and design an appropriate response to its potential weapons of mass destruction (WMD) program."[31]

Cyber CWMD operations, similar to cyber SR, also seem to leverage economy of manpower and resources. The (STUXNET) malware most likely impaired Iran's nuclear making capabilities as much as a DA attack by Israel would have.[32] If the same effects in cyberspace are achieved without putting boots on the ground, planes in the air or causing civilian casualties, then further use of cyber weapon systems requires strong consideration.

As a counterpoint, the broader costs of relying only on the cyber domain require further analysis. SOF have always placed a strong focus on the human domain, and without putting boots on the ground, this element may be lost. Only so much access can be garnered from afar. At some point, the implementation of human intelligence and technical implantation of cyber technologies may necessitate boots on the ground. For instance, with STUXNET, the Iranian nuclear facility was air gapped from the open network. If someone was not physically available to inject malicious code via a USB drive into the SCADA system, the STUXNET program may have not succeeded.

4. Counterterrorism and Hostage Rescue and Recovery

Counterterrorism (CT) is defined in JP 3–05 as, "activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals."[33] The joint publication also defines "Hostage Rescue and Recovery (HRR) as a personnel recovery method used to recover isolated personnel who are specifically

[31] Philip M. Forbes, "Son of SPECOPS: Rethinking the Nature and Operationalization of Cyberspace." Naval War College Newport Rhode Island Joint Military Operations Department, 2012, 9.

[32] Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press, 2012), State on State Cyber Attacks, 155.

[33] U.S. Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05, Washington, DC: Joint Chiefs of Staff, April 18, 2010.

designated as hostages."[34] Because the other supporting core activities feed into CT/HRR, their application to the cyber domain as discussed below also supports CT/HRR.

D. SPECIAL WARFARE CORE ACTIVITIES

1. Counterinsurgency

The Department of Defense defines counterinsurgency (COIN) as "comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes."[35] Though COIN falls within the Special Warfare umbrella it can also fall under Surgical Strike. The COIN example of surgical strike may include DA. COIN is the current focus for military operations in Iraq, Afghanistan, and other areas of insurgent activity. Special Warfare at its root is deeply ingrained in COIN, and vary rarely do COIN operations necessitate the application of Surgical Strike.

Applying cyber operations to COIN and Special Warfare, SOF could remotely, via the Internet, train indigenous populations on how to employ Unmanned Arial Vehicles (UAV's) to observe, engage, and disband gatherings as part of cyber-enhanced populace control measures.[36] Cyber COIN could also instruct populations on how to construct crowdsourced, geo-tagged, and non-standard databases for potential population centric operations.[37] These operations can be used to gradually damage the opposition's quality of life through cyber centric targeted operations and "tactics rather

[34] Ibid.

[35] Ibid.

[36] Patrick Duggan, "Man, Computer, and Special Warfare." APAN. January 4, 2016. Accessed May 04, 2016. https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog/archive/2016/01/08/man-computer-and-special-warfare.

[37] Patrick Duggan, "Man, Computer, and Special Warfare." APAN. January 4, 2016. Accessed May 04, 2016. https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog/archive/2016/01/08/man-computer-and-special-warfare.

than quick, high profile battles with decisive results."[38] Cyber COIN operations also form an umbrella to the more technical core activities, such as UW and MISO.

2. Unconventional Warfare

Unconventional Warfare is defined in JP 3–05 as, activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area."[39] Special Forces mission and functions are organically derived from Unconventional Warfare. UW is the standard method to averting future significant military conflicts. USSOCOM's core activity, Unconventional Warfare (UW), is built on the foundation of other core activities working by, through, and with indigenous or surrogate forces to overthrow an occupying or government force."[40]

COL Duggan theorizes that the application of cyber UW appears to be limitless. Centered on the idea of resistance movements, Special Operators could utilize 3-D printing technology to manufacture equipment and repair parts for resistance groups' guerillas and members of their underground support networks.[41] Cyber UW operations could empower resistance groups through 3-D technology by manufacturing computers, weapons, munitions, engines, UAVs, and IEDs.[42] Other applications of cyber UW may include the utilization of human, informational, physical, and intelligence networks to target an occupying force's logical and physical computer network.[43] Similar to the use of precision guided technology, the suite of cyber tools available can target precise

[38] Ibid.

[39] "Joint Publication 3-05, Joint Special Operations." Apr 2011. Council on Foreign Relations. Dec 2016, XI.

[40] Ibid.

[41] Patrick Duggan, "Man, Computer, and Special Warfare." APAN. January 4, 2016. Accessed May 04, 2016. https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog/archive/2016/01/08/man-computer-and-special-warfare.

[42] Ibid.

[43] Ibid.

elements of an information network while minimizing collateral damage.[44] Realizing the unlimited potential of UW operations, cyber UW can work with the private sector to improve a tactic domestically while simultaneously denying an adaptive adversary a "technological advantage through counter UW constructs."[45]

Unfortunately, UW is not always a palatable concept with interagency partners and embassy staffs because of the mission to overthrow an occupying force, but the idea of cyber enabled UW may alleviate undue stress. Conceptually, cyber UW builds "human, physical, intelligence, and information infrastructures on social media platforms with cyber tools and advanced techniques without putting boots on the ground."[46] The theory is collection from afar, which allows USSOCOM the ability to conduct core activity while all parties within the USG maintain the ability to monitor operations. Small technological inputs, as these not only build trust within the interagency, but they may also set the conditions for operations in other theaters of conflict.

3. Foreign Internal Defense

Foreign Internal Defense (FID) is defined as the "participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security."[47] FID operations typically occur in a peacetime environment and commonly are Joint Capability Exchange Training (JCET) exercises. The aim is to empower "HN forces to maintain internal stability, counter subversion and violence, and address root causes of instability."[48]

[44] Ibid.

[45] Ibid.

[46] Patrick Michael Duggan, "Strategic Development of Special Warfare in Cyberspace," Joint Force Quarterly 79 (2015): 46-53.

[47] "Joint Publication 3-05, Joint Special Operations." Apr 2011. Council on Foreign Relations. Dec 2016, XI.

[48] Ibid., II-11.

Similar to cyber UW, cyber-enabled FID is a cheap and low-cost program that can empower indigenous populations through minimal technology and most importantly minimal loss of life.[49] From operations, such as conducting virtual reality weapons training, to providing real-time guidance through virtual uplinks, as with UW, the applications of cyber technology are limitless. In areas of low or no connectivity, the distribution of low-cost operating systems and devices, such as the Raspberry Pi, could facilitate "a wide-array of communication, command, and control, as well as mapping functions."[50] Virtual reality technology could also enable the inclusion of robotic technology to assist in the training and ultimate employment of host nation forces.

4. Security Force Assistance

The Department of Defense's National Strategy for Cyberspace's centrally highlights building (cyber) partner capacity in key regions."[51] The task of Building Partner Capacity (BPC) or more appropriately termed "Security Force Assistance (SFA) is defined as the Department of Defense activities that contribute to unified action by the U.S. Government to support the development of the capacity and capability of foreign security forces and their supporting institutions."[52] The DOD's Cyber Strategy states, "The Defense Department will work regularly with other agencies of the U.S. Government, to include the Department of State, in building partner capacity."[53]

[49] Patrick Duggan, "Man, Computer, and Special Warfare," APAN. January 4, 2016. Accessed May 04, 2016. https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog/archive/2016/01/08/man-computer-and-special-warfare

[50] Ibid.

[51] "Department of Defense Strategy for Operating in Cyberspace," National Institute for Standards in Technology, July 2011, accessed December 15, 2016, csrc.nist.gov/groups/SMA/ispab/.../DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[52] U.S. Joint Chiefs of Staff. *Foreign Internal Defense*, Joint Publication 3-22, Washington, DC: Joint Chiefs of Staff, July 12, 2010.

[53] "Department of Defense Strategy for Operating in Cyberspace," National Institute for Standards in Technology, July 2011, accessed December 15, 2016, csrc.nist.gov/groups/SMA/ispab/.../DOD-Strategy-for-Operating-in-Cyberspace.pdf.

The Foreign Assistance Act of 1961 designates[54] the Department of State (DOS) as the primary director of SFA and the DOD in support. As currently delegated within the DOD, SFA is sponsored by the Department of the Army and USSOCOM.[55] As Harry Yarger, military scholar and author of *Building Partner Capacity*, commented on the importance of SOF in a BPC (SFA) strategy, "Special Operations Forces (SOF) are instrumental components in the pursuit of a successful BPC policy."[56] Though SOF are not experts in cyber SFA nor do they have an exemption to Public Law 87–195, they do have a unique position within a large number of embassy country teams. SOF are embedded in multiple embassies across the world as Military Liaison Elements (MLE) that are designed to work side-by-side with country teams to achieve a unified approach to shaping operations. This unique position may serve as an advantage point when the DOD attempts to implement a cyber SFA strategy.

5. Foreign Humanitarian Assistance

Foreign Humanitarian Assistance (FHA) is defined by the DOD as, " the activities conducted outside the United States and its territories to directly relieve or reduce human suffering, disease, hunger, or privation."[57] FHA is a cornerstone activity that builds trust with partner nations and highlights the fluidity and adaptability of USSOCOM. Whether responding to the earthquake in Haiti or a typhoon in the Philippines, FHA operations are important not only to national security but also to the preservation of human life.

Unfortunately, one of the biggest issues when conducting FHA operations is quick and simple collaboration. The problem is that the Department of Defense Information Network (DODIN) is not available for outside organizations. Another issue is that the classification levels of Confidential, Secret, and Top Secret, weigh too heavily

[54] Harry R. Yarger, *Building Partner Capacity*, No. JSOU-R-15-1. Joint Special Operations University MacDill Airforce Base FL, 2015.

[55] Ibid.

[56] Ibid.

[57] U.S. Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05. Washington, DC: Joint Chiefs of Staff, April 18, 2010.

on the concept of secrecy, which ultimately hinder network availability. Without the ability to communicate across all organizations, FHA operations may falsely identify USSOCOM as a secretive organization with a clandestine objective.

Though USSOCOM is not tasked to directly address FHA connectivity issues, the rapid response capability of USSOCOM typically means they are first boots on the ground and therefore should be prepared. To address this cyber capability gap, USSOCOM, in times of crises, could build an ad-hoc civilian network that promotes collaboration and availability. This quick response cyber unit could hastily set up a network that allows all parties to communicate on an open and dynamic basis while protecting confidential information. USSOCOM could develop a rapidly deployable unit composed of network experts who are capable of immediately building and supporting a multi-stakeholder network. To remove the outside perception of military bias, network operations could immediately include non-governmental organizations and host nation stakeholders.

6. Military Information Support Operations

Military Information Support Operations (MISO)/Psychological Operations (PSYOP) are defined in JP 3–05 as “the planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator’s objectives.”[58] “The purpose of MISO is to induce or reinforce foreign attitudes and behaviors favorable to the joint force commander’s objectives.”[59] “USSOCOM is assigned to develop Military Information Support Operations (MISO) capabilities in support of the Joint Staff’s

[58] U.S. Joint Chiefs of Staff. *Special Operations*. Joint Publication 3-05. Washington, DC: Joint Chiefs of Staff, April 18, 2010.

[59] “Special Operations Forces Reference Manual,” Federation of American Scientist, June 2015, accessed December 15, 2016, https://fas.org/irp/agency/dod/socom/ref-2015.pdf.

information operations (IO) responsibilities and provide support to combatant commanders for theater MISO planning and execution."[60]

Cyber operations can "leverage sympathetic privateers and vigilantes, as well as employ false flag efforts to create believable deceptions in cyberspace" over a prolonged period.[61] These operations, all conducted from afar, provide an opportunity for USSOCOM to conduct Special Warfare without ever putting boots on the ground. SOF provides access to and the ability to influence populations where conventional U.S. force presence is not warranted.

Conducting cyber-centric operations in support of MISO may create a non-resource intensive and cost effective environment that may facilitate operations on a much larger scale than traditional non-cyber centric MISO. As a real world example, cyber mastermind and current Russian Chief of Staff, General Gerasimov, believes wholeheartedly in persistent cyber engagements in support of MISO, "Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals."[62]

7. Civil Affairs Operations

The Department of Defense defines Civil Affairs Operations (CAO) as:

> actions planned, executed, and assessed by civil affairs forces that enhance awareness of and manage the interaction with the civil component of the operational environment; identify and mitigate underlying causes of instability within civil society; or involve the application of functional specialty skills normally the responsibility of civil government.[63]

[60] Ibid.

[61] Patrick Duggan, "Man, Computer, and Special Warfare," APAN. January 4, 2016. Accessed May 04, 2016. https://community.apan.org/wg/tradoc-g2/mad-scientist/b/weblog/archive/2016/01/08/man-computer-and-special-warfare.

[62] Patrick Michael Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly* 79 (2015): 47.

[63] U.S. Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05, Washington, DC: Joint Chiefs of Staff, April 18, 2010.

USSOCOM's incorporation of the cyber domain within the core activity CAO may present a possible opportunity to address this issue through the engagement strategy of addressing partner nation cyberspace vulnerabilities. Cyber enabled CAO could assess partner nation infrastructure for potential zero day vulnerabilities or conduct proxy cyber-attack exercises to test the partner nation's capability to conduct cyber defense. The combined exercises, executed under the "red team / blue team" methodology, could uncover underlying weakness that may potentially cripple a partner nation's ability to provide its civilian core the essential civil services they need to survive.

Viewed through a different light, cyber vulnerability reduction allows the partner nation the opportunity to address potential issues that may promote a violent extremist organization's (VEO) ability to recruit or mobilize. Forbes, military author and cyber academic states, "Such expansion may include partnering with governments and non-governmental organizations (NGOs) to ensure that global allies in defense and commerce can maintain the network architecture that facilitates daily social and governmental functions."[64]

E. CONCLUSION AND WAY AHEAD

This chapter examined how USSOCOM could employ cyber operations in support of special operations. While analyzing the macro and micro levels of special operations, it showed that the application of cyber techniques, tactics, and procedures present a possible avenue to supplement, or in some cases replace, traditional special operations. Operations conducted from afar allow for greater risk management within the realm of manpower but may limit human domain capabilities. The next chapter examines whether USSOCOM can rely on USCYBERCOM for its cyber operations or if it needs to build an internal cyber capability in order to take full advantage of the possibilities offered by cyberspace for supporting special operations.

[64] Philip M. Forbes, "Son of SPECOPS: Rethinking the Nature and Operationalization of Cyberspace" (Final Paper, Naval War College Newport Rhode Island Joint Military Operations Department, 2012).

III. MEETING USSOCOM'S MISSION THROUGH CYBER OPERATIONS

This chapter lays the foundation for how best USSOCOM can meet its mission requirements through the incorporation of cyber operations. The chapter first describes how the DOD organizes for cyber operations through USCYBERCOM and how USCYBERCOM serves USSOCOM. It then examines nine criteria to determine if USCYBERCOM's support is sufficient or if USSOCOM should instead develop an internal cyber capability. Specific focus is applied to cyber mission, organization, U.S. Code Title authorities, budget, and relevance. The chapter concludes with an overall assessment.

A. CURRENT U.S. CYBER ORGANIZATION

Secretary of Defense Robert Gates, focusing on military cyberspace operations, ordered the creation of USCYBERCOM in 2009. The command was established not as a Combatant Command (COCOM) but as a subordinate command. USCYBERCOM is subordinate to the United States Strategic Command (STRATCOM). USCYBERCOM combined multiple cyber and information military components within the DOD's network security capability and unified them at the command's Fort Meade headquarters.[65] Secretary Gates further directed that the commander of USCYBERCOM would be the director of the National Security Agency (NSA).[66] Although USCYBERCOM attained full operational capability (FOC) in 2010, it was not expected to reach its designated strength until the end of 2018.[67]

The mission statement for USCYBERCOM states,

[65] Tanner Leah, "Examining Cyber Command Structures" (master's thesis: Naval Postgraduate School , 2015).

[66] Ibid.

[67] Mark Pomerleau, "Cyber Command Getting Closer to Full Deployment—Defense Systems," Defense Systems, June 23, 2016, https://defensesystems.com/articles/2016/06/23/cyber-command-gets-closer-to-full-deployment.aspx.

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks; and prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace and deny the same to our adversaries.[68]

In this role, USCYBERCOM is required to provide defense, both physical and logical, to the Department of Defense Information Network (DODIN); provide cyber support to the Geographic Combatant Commands (GCCs); and provide, in time of need, cyber support to the USG.[69] Figure 3 visually describes the USCYBERCOM mission as it relates to unit imperatives and enablers.

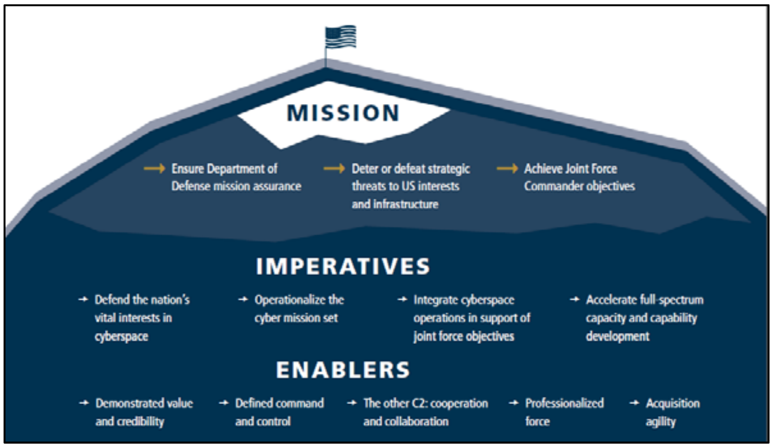

MISSION
→ Ensure Department of Defense mission assurance
→ Deter or defeat strategic threats to US interests and infrastructure
→ Achieve Joint Force Commander objectives
IMPERATIVES
→ Defend the nation's vital interests in cyberspace
→ Operationalize the cyber mission set
→ Integrate cyberspace operations in support of joint force objectives
→ Accelerate full-spectrum capacity and capability development
ENABLERS
→ Demonstrated value and credibility
→ Defined command and control
→ The other C2: cooperation and collaboration
→ Professionalized force
→ Acquisition agility

Figure 3. USCYBERCOM Mission.[70]

[68] U.S. Cyber Command, *Beyond the Build, Delivering Outcomes Through Cyberspace*, Washington, DC: Department of Defense, June 3, 2015.

[69] Tanner Leah, "Examining Cyber Command Structures" (master's thesis, Naval Postgraduate School , 2015).

[70] Mike Rodgers, "Beyond the Build, Delivering Outcomes Through Cyberspace," June 3, 2015. Accessed December 14, 2016. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf.

In his March 2015 thesis on cyber command structures, Tanner Leah noted that,

> USCYBERCOM is currently just over 6,000 billets (drawn from the services), while the services will by 2016 have nearly 43,000 total personnel (active duty service members, civilians, and contractors: Army: 21,000, Air Force: 5,400, Navy: 15,300, Marines: 1,000) dedicated to cyber missions, such as DODIN operations and offensive and defensive cyber operations (DCO).[71]

While unlikely to be as large as the Air Force at its founding, a cyber force would likely be larger than the roughly 43,000 personnel envisioned by the end 2016.[72] ADM Stavridis, among others, has advocated for a standalone cyber force, independent and equal to the standing components of the," Navy, Air Force, and Marine Corps.[73]

USCYBERCOM is centered on three "focus areas: defending the DODIN, providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber-attacks."[74] USCYBERCOM created cyber mission forces with the sole purpose of addressing each focus area in detail. These forces are organized into three distinct types of teams corresponding to the three focus areas: Cyber Protection Forces (CPF), developed to protect the DODIN; Combat Mission Forces (CMF), assigned to GCCs for offensive and defensive cyber missions; and National Mission Forces (NMF), developed for defending critical national infrastructure. To populate the required force, USCYBERCOM is still formulating the proper design for the optimal team composition. They are in the process of defining the training requirements and essential qualifications to ensure they are meeting the GCCs' operational needs.

[71] Tanner Leah, "Examining Cyber Command Structures" (master's thesis: Naval Postgraduate School , 2015).

[72] Ibid.

[73] James Stavridis, "USNI Logo," Time for a U.S. Cyber Force. January 2014. Accessed September 24, 2016. http://www.usni.org/magazines/proceedings/2014-01/time-us-cyber-force.

[74] "U.S. Cyber Command," March 2015. Accessed September 24, 2016. https://www.stratcom.mil/factsheets/2/Cyber_Command/.

By 2018, USCYBERCOM is expected to field 133 cyber teams in total.[75] As of June 22, 2016, "the command's deputy commander, Lt. Gen. James McLaughlin, told the House Armed Services Committee there are 46 teams at full operational capacity and 59 at initial operational capacity leaving, 28 still to go."[76] Even after USCYBERCOM has filled all 133 teams, only 27 will be assigned to GCCs.[77]

USCYBERCOM personnel assigned to the service cyber organizations are under the administrative control (ADCON) of each of the cyber components, while personnel assigned to USCYBERCOM fall under USCYBERCOM's authority.[78] However, USCYBERCOM retains operational control (OPCON) over all cyber personnel who reside within USCYBERCOM, no matter their originating component. USCYBERCOM provides Cyber Protection Teams to the GCCs; once assigned, the GCCs provide tactical control (TACON) over their employment. Figure 4 is a graphical representation of USCYBERCOM and its relationship to the GCCs and USSTRATCOM. Of note, because USCYBERCOM is not a unified command, USSTRATCOM interfaces with the GCCs on behalf of USCYBERCOM.

[75] Mark Pomerleau, "Cyber Command Getting Closer to Full Deployment—Defense Systems." Defense Systems (May 23, 2016). Accessed September 27, 2016. https://defensesystems.com/articles/2016/06/23/cyber-command-gets-closer-to-full-deployment.aspx.

[76] Ibid.

[77] Ellen Nakashima, "Pentagon Cyber Unit Wants to 'get inside the Bad Guy's Head,'" *Washington Post* (April 19, 2016). Accessed October 07, 2016. http://www.washingtonpost.com/news/checkpoint/wp/2014/06/19/pentagon-cyber-unit-wants-to-get-inside-the-bad-guys-head/.

[78] Tanner Leah, "Examining Cyber Command Structures" (master's thesis: Naval Postgraduate School, 2015).

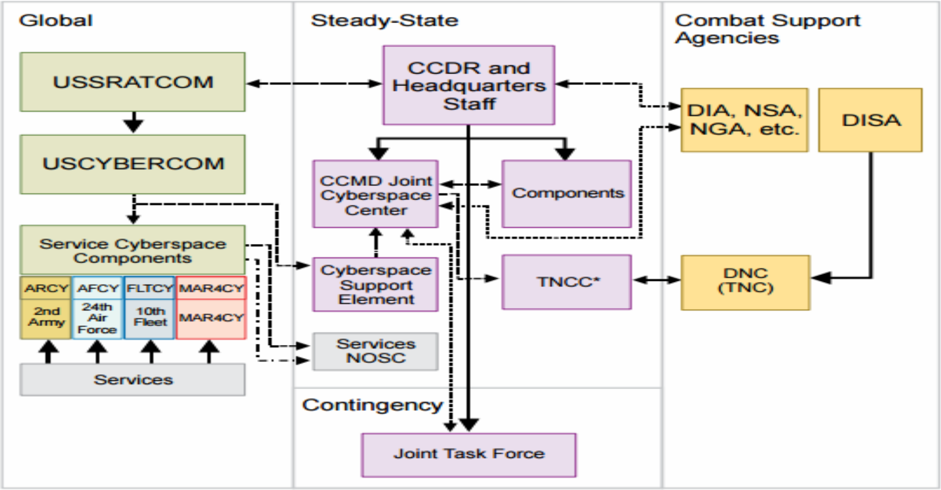


Figure 4. USCYBERCOM Organizational Support Structure.[79]

B. HOW USCYBERCOM CURRENTLY SERVES USSOCOM

As of 2016, USSOCOM does not possess an internal cyber component and is reliant upon USCYBERCOM for almost all operational support. Though there has yet to be an official definition of what the cyber operational support will look like (size and capacity), as noted above USCYBERCOM is planning to field 133 cyber mission teams, 27 of which will be allocated to the COCOMs.’[80][81] Although how these 27 teams will be allocated to the COCOMs is not definitive, given that there are seven GCCs, this is roughly four teams per GCC, assuming equal distribution.

The future teams assigned to support USSOCOM may be divided along two lines of effort: 1) cyber mission forces for preemptive/unprovoked cyber operations, and 2) cyber protection forces for securing USSOCOM’s network. For the sake of argument, if

[79] Joint Publication 3-12 (R), *Cyberspace Operations*. 5 February 2013.

[80] Paul Rosenzwelg, “The New Face of Law and Cyber Warfare,” LawFare (October 18, 2016). Accessed October 28, 2016. https://www.lawfareblog.com/new-face-law-and-cyber-warfare.

[81] Ellen Nakashima, “Pentagon Cyber Unit Wants to ‘get inside the Bad Guy’s Head,’” *Washington Post*. April 19, 2014. Accessed October 07, 2016. http://www.washingtonpost.com/news/checkpoint/wp/2014/06/19/pentagon-cyber-unit-wants-to-get-inside-the-bad-guys-head.

USSOCOM is assigned four cyber teams, one of which is dedicated to defending the network within USSOCOM, that leaves three teams to cover six Theater Special Operations Commands (TSOCs). Considering that in total, the TSOCs have operations in over 100 countries, which are also subdivided into multiple component special operations units, the cyber support from USCYBERCOM may be inadequate.[82]

Of the undetermined cyber forces provided to USSOCOM, the researcher assumes they will serve in a dual-hatted role as they provide cyber support to USSOCOM, as a traditional unified command and uniquely support the TSOCs and their regionally focused special operations. The TSOCs may be at an advantage as a supporting command because they will be both supported by the COOCOM? and USSOCOM. Conversely, it is also possible the TSOCs do not receive cyber force augmentation as a GCC supporting command. Considering the precious nature and limited supply of cyber mission forces, the TSOCs should not conclude GCC cyber support is a guaranteed

C. CYBER SUPPORT CRITERIA

In order to assess USCYBERCOM's cyber support to USSOCOM and whether USSOCOM would be better served by an internal cyber element, the researcher identified and analyzed nine criteria. These range from objective factors such as budgets and U.S. Code authorities to subjective elements such as culture and mindset. After discussing each of these, the chapter will give an overall assessment.

1. Mindset and Culture

The first criterion is mindset and culture. The reason mindset and culture was selected as an evaluation criterion is because USSOCOM's cyber operations will require extensive expertise in the cultural nuances of a myriad of different operating environments.

[82] Of note the exact number of cyber teams required may necessitate further analysis on the behalf of USSOCOM but an initial estimate of ten teams is discussed below under the heading "operational need."

Attribution of cyber operations to the country or organization of origin is of big concern when developing cyber weaponry. As an example, consider STUXNET. Initial speculation about who conducted the operation led to Israel, in part because of a word found in the code, "Myrtus."[83] Myrtus is the Hebrew translation of the English word Esther, and Esther is from the Old Testament (Torah). In order to prevent the attribution of sensitive cyber programs, USCYBERCOM will require linguistically and culturally knowledgeable cyber operators that know to avoid such disclosures.

Culture is not only important externally to the organization, but also within. The internal culture or mindset of USSOCOM is equally as important to the mission. USSOCOM carries a unique culture that is built on trust, cohesion, unity, and understanding. A critical component of the USSOCOM internal culture stems from the highly selective nature of the unit. USSOCOM is staffed with some of the best Soldiers, Airmen, Marines, and Sailors the military has to offer. Cyber forces in support of USSOCOM will have to fit this requirement or they may be subject to marginalization.

From the standpoint of the SOF cybertheorist Patrick Duggan, SOF specifically operates with a mindset that is capable of addressing "ambiguous associations between adversaries, computers, and data, while minimizing risks to force and mission."[84] The ability of SOF to operate with a minimal footprint while applying exact force applies to the entire gamut of human based warfare, including cyber war.[85]

Duggan notes that "cyber SOF could tap into indigenous revolutions, resistance movements, and insurgencies, as well as harness the human factors of techno-social interaction, whether operating on the ground with them or while continents away."[86] Cultural sensitivity is clearly critical for the success of these operations. Ultimately, cyber

[83] John Markoff and David E. Sanger, "In a Computer Worm, a Possible Biblical Clue," *The New York Times*, September 29, 2014, accessed December 15, 2016, http://nyti.ms/1H3bhI8.

[84] Patrick Duggan, "Why Special Operations Forces in U.S. Cyber-Warfare?" *The Cyber Defense Review*. January 8, 2016. Accessed May 18, 2016. http://www.cyberdefensereview.org/2016/01/08/why-special-operations-forces-in-us-cyber-warfare/.

[85] Ibid.

[86] Ibid.

SOF could employ the elements of Special Warfare to slowly change an adversary's organization without ever physically entering it.

Though USCYBERCOM may one day become capable of conducting these cyber SOF niche operations, without the immediate blending of organizational cultures between USCYBERCOM and USSOCOM, the operational gap may never be bridged. SOF-established human networks are already standing worldwide and potentially capable of implementing cyber technologies. Without SOF intervention, many of the capabilities described in the preceding paragraph may never have the opportunity to materialize - especially in time-sensitive environments.

Cyber operators have many similarities that run parallel to the culture ingrained into the special operations community. Similar to the SOF community, cyber operators will require regional, cultural, and language training.[87] They will need to understand a cyber adversary's dialect, work patterns, coding nuances, and methods of employment to fully understand the second and third order of cyber effects. As exemplified by STUXNET and the decoding of the worm, if the originator's code contains information, i.e., cultural references or language, that is not particular to the region of employment, an objective of operating anonymously may not be met.

With respect to the criteria of Mindset and Culture, USCYBERCOM, as currently structured, may not be able to meet the unique cultural needs of USSOCOM. If USCYBERCOM were to formalize a cultural and language training program and better mold its operators to the unique mindset of USSOCOM, they may be able to bridge this requirement gap. USCYBERCOM may one day mature to the point of including culture and language training similar to USSOCOM's training model, but in the interim if USSOCOM requires a culturally astute cyber force, USSOCOM will be required to provide the training.

[87] Stew Magnuson, "Do Cyberwarriors Belong at Special Operations Command? *National Defense Magazine.* August 01, 2011. Accessed April 02, 2016. http://www.nationaldefensemagazine.org/archive/2011/August/Pages/DoCyberwarriorsBelongatSpecialOperationsCommand.aspx.

2. Operational Cyber Need

Operational cyber need is a critical factor when determining the suitability of cyber support to USSOCOM. SOF are deployed in support of the GCCs in an atypical fashion, unique to each theater. The TSOC requirements in PACOM tend to vary from the TSOC requirements in CENTCOM. Furthermore, regional focus tends to shift based on guidance from USSOCOM’s Global Campaign Plan for Special Operations. The factors of operational cyber need may greatly influence the cyber footprint required for special operation’s missions. Cyber forces supporting USSOCOM will need the ability to dynamically re-task from each theater to support the global plan provided by USSOCOM. Cyber forces will also require the ability to surge as needed in support of specific national special objectives.

As noted earlier, USCYBERCOM will field 27 Combat Mission Teams for distribution among all COCOMs. As of January 2014, USSOCOM was deployed to over 100 countries and multiple SOF elements were supporting each country. Depending on the final cyber team size (currently estimated around 40–70)[88] and scope of responsibility, USSOCOM will most likely require a robust cyber support element for each TSOC and several more at the command level. Without further analysis, it is difficult to say how many teams USSOCOM could effectively deploy, but this researcher estimates that USSOCOM could use at least 10 teams.

If USCYBERCOM desires to bridge this operational gap, they would have to develop more cyber forces or shift priorities away from other COCOMs. The exact number of cyber forces requires further analysis on the behalf of USSOCOM and the TSOCs, but based on the sheer mission load, the current number of forces under the equal COCOM distribution model may not meet the operational requirement.

[88] Paul Rosenzwelg, “The New Face of Law and Cyber Warfare.” LawFare. October 18, 2016. Accessed October 28, 2016. https://www.lawfareblog.com/new-face-law-and-cyber-warfare.

3. Cyber Warfare is Human Warfare

The concept of human warfare is a critical criterion when evaluating USCYBERCOM's cyber support to USSOCOM. To be sure, the cyber domain is human warfare no matter the operational environment, conventional or special operations, and therefore not specific to the requirements of USSOCOM. However, cyber warriors in support of USSOCOM will require the ability to mobilize as part of an asymmetric strategy against foreign adversaries. Duties may include airborne operations or clandestine infiltration into enemy occupied territory.

The DOD has designated SOF as the premier force / subject matter experts for engagements in the human dimension. With this in mind, there appears to be a strong relationship to the inclusion of cyber and special operations. It is highly unlikely all that all cyber operations require SOF, but cyber operations that are politically sensitive in nature or require a high degree of human interaction are better suited for SOF. Of course, not all cyber operations are inherently sensitive to the political environment. For instance, if a conventional unit conducts a DA cyber-attack, as discussed in Chapter II, on a low level ISIS bomb maker, it is highly unlikely the effects will contain political ramifications.

According to Duggan, "in spring 2014, Russia successfully demonstrated its new understanding of how to integrate (cyber) asymmetric technology into unconventional warfare (UW) operations by supporting paramilitary separatists in eastern Ukraine."[89] Countries such as Iran and Russia successfully employ human based cyber-warfare through the pairing of SOF and Special Warfare. Iran and Syria have integrated a strategy to incorporate cyber-SOF and how to leverage this…potential within the asymmetric nature of conflict."[90]

[89] Patrick Duggan Michael, "Strategic Development of Special Warfare in Cyberspace."

[90] Patrick Duggan, "Why Special Operations Forces in U.S. Cyber-Warfare?" *The Cyber Defense Review*. January 08, 2016. Accessed April 02, 2016. http://www.cyberdefensereview.org/2016/01/08/why-special-operations-forces-in-us-cyber-warfare/.

While understanding that the cyber domain is human-based warfare, no matter the operating environment, the unique human-based requirements created by USSOCOM may leave USCYBERCOM in an operational shortfall unless USCYBERCOM adds more human dimension-based capability into its USSOCOM specific cyber forces. USCYBERCOM may also need to add advanced capabilities into its force structure that allow cyber operators the opportunity to directly embed with SOF.

4. Integration with USSOCOM Operations

The integration of cyber forces into USSOCOM is critical because unity of command is a top priority for the USSOCOM commander. Relationships are important to USSOCOM, therefore cyber forces would have to maintain a habitual and lasting relationship with the command with little organizational bureaucracy. This cyber-support relationship would need to be responsive and dynamic, continually supporting the fluid nature of USSOCOM.

Fitzgerald and Wright believe that USCYBERCOM is inefficiently organized to provide support to USSOCOM's worldwide special operation requirements.[91] They believe that while in a supporting role, USCYBERCOM's preservation of cyber employees within the command prohibits USSOCOM from truly achieving unity of command.[92] "For SOF cyber operations to be successful, it may require an in-house cyber component or organization that would ultimately serve as a full member of the USSOCOM command team, which is noticeably different from the current organization of a separate joint functional component at USCYBERCOM."[93] Because of this

[91] Ben Fitzgerald and LtCol Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control*. Disruptive Defense Papers: Center for a New American Security, April 2014. Accessed December 14, 2016. http://www.cnas.org/sites/default/files/publications-pdf/CNAS_DigitalTheaters_FitzGeraldWright.pdf.

[92] Ibid.

[93] Ben Fitzgerald and Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control*, Disruptive Defense Papers: Center for a New American Security, April 2014. Accessed December 14, 2016. http://www.cnas.org/sites/default/files/publications-pdf/ CNAS_ DigitalTheaters_FitzGeraldWright.pdf.

USSOCOM may require a single, local cyber commander to ensure unity of effort across all GCCs.[94]

With cyber forces allocated from USCYBERCOM to USSOCOM on a lease status, USSOCOM never achieves full operational control. This operational gap could be alleviated if USCYBERCOM were to provide a cyber command representative to USSOCOM as command to command liaison. Another option is for USCYBERCOM to provide forces to USSOCOM under an OPCON status.

5. Need for Commanders within Reach

Based on the current TSOC structure, the TSOCs will most likely require a cyber mission commander within the chain of command. In order to meet this criterion, USCYBERCOM will need to provide cyber forces to the TSOC in an OPCON role—ultimately allowing the TSOC commander the opportunity to direct and control cyber forces within the command.

If USSOCOM has to coordinate with a distant USCYBERCOM commander, this may be less effective than if USSOCOM has an internal cyber element. Technologies such as Adobe Connect, Tanberg, and Skype make worldwide interactions easier than ever, but nothing can replicate the value in face to face interactions, as demonstrated by the success of the technology networks of Silicon Valley.[95] Anecdotally, most commanders are as interested in the supporting relationship of Operational Control (OPCON)—the capacity to physically direct and discipline a subordinate commander—as they are with any of the official command relationships.[96] An intra-SOF cyber command will have a higher kinship for the USSOCOM commander and be inclined to respond to that commander’s requirements foremost. If the cyber team or component commander to whom the GCC interacts with is neither a vested commander nor easily

[94] Ibid.

[95] Russell, Cherry, Andrew Campbell, and Ian Hughes, “Research: Ageing, social capital and the Internet: Findings from an exploratory study of Australian ‘silver surfers’.” *Australasian Journal on Ageing* 27, no. 2 (2008): 78-82.

[96] Ibid.

reachable, then the GCC will rely less on worthwhile cyber aptitudes and relapse to traditional means of waging war.[97]

Of all people on the battlefield, the TSOC commander knows best where to employ special operations effects. The commander may not be the cyber subject matter expert, but he or she understands how to leverage a cyber warrior's expertise to support, replace, or reinforce SOF capabilities. The commander has the best understanding of the structures and practices unique to SOF and their operations.[98] SOF peculiar cyber teams would enjoy a communal conviction and mission empathy with their SOF comrades.[99]

Considering this criterion, the operational, administrative, and tactical control of cyber missions is a critical concept when determining the benefit or failure of cyber forces, not only the TSOCs, but also USSOCOM writ large. In order to meet the criterion set forth, USCYBERCOM will need to provide the USSOCOM with full autonomous control of its assigned cyber forces. At this time, USCYBERCOM operates on an OPCON status, which greatly limits the TSOC commander's directional power.

6. Procurement Advantages

The ever-changing operational environment in which SOF operate require a supporting cyber force that is capable of rapid procurement. Cyber forces in support of USSOCOM must possess the ability to assess operational environment quickly and develop technologies that best address the current threat.

Building an intra-SOF cyber organization will give those cyber forces SOF-unique procurement means for cyber capability generation, innovation, funding, and development. USSOCOM is the exclusive stakeholder for Major Force Program-11 (MFP) funding. MFP-11 funding, separate from the traditional service component MFP-3

[97] Ibid.

[98] Ben Fitzgerald and Parker Wright, *Digital Theaters: Decentralizing Cyber Command and Control*. Disruptive Defense Papers: Center for a New American Security, April 2014. Accessed December 14, 2016. http://www.cnas.org/sites/default/files/publications-pdf/ CNAS_ DigitalTheaters_FitzGeraldWright.pdf.

[99] Ibid.

funding, allows the organization the opportunity to conduct rapid fielding and procure SOF peculiar equipment. If a cyber organization is housed within USSOCOM, it will retain the ability to procure service specific equipment under MFP-3 and SOF peculiar items under MFP-11. This allows the intra-SOF cyber command the ability to essentially leverage all forms of funding and field cyber related capabilities at nearly double the rate of MFP-3.

USCYBERCOM may be unable to meet the rapid acquisition requirements as identified by USSOCOM. The hierarchical procurement nature of USCYBERCOM and MFP-3 funding prevents the command from rapidly meeting evolving SOF requirements. USCYBERCOM may be able to bridge this gap if they are granted rapid fielding authorities, such as included in MFP-11, but until then they are subjugated to longer capability development timelines.

7. Control of Cyber Forces

The current cyber structure is based on the premise that all cyber functions within the Department of Defense should be conducted and controlled by USCYBERCOM. Though the centralized control of cyber forces might make sense today, it may not fully take into account the future of warfare.

Cyber operations, specifically, and more broadly the cyber domain, are among one of the most critical factors in combat. Maintaining and directing all cyber operational forces from USCYBERCOM appears to be conducive for the moment but has yet to be tested against an alternative. Alternative cyber force models include: decentralized forces, autonomous forces, interagency forces, or multi-national forces. These alternate forms may one day serve as attractive alternatives to the current USCYBERCOM model.

Another area of analysis is the complex nature of cyber warfare and the difficulty of containing cyber effects on the intended target. An example of failing to oversee effects based operations is exemplified through IO (Information Operations) fratricide. This term is used to describe a situation in which one organization marginalizes an IO target while another bolsters it. The two efforts oppose each other and create an unfavorable position for both organizations. USCYBERCOM's one-stop cyber structure may create an environment that allows proper command and control over each cyberspace munition; ultimately preventing opposing efforts and ensuring unity of effort. The ability to vet, measure, contain and control cyber munition under one command greatly reduces the possibility of cyber fratricide. However, as the cyber fight continues to progress, the sheer volume of cyber-operations may become too much for one command to handle just as no single command handles all air operations.

8. Title 10/50

Title 10/50 authorities are critical to conducting cyber operations. Cyber operations are sometimes referred to as inherently covert and therefore necessitate USCYBERCOM's involvement under Title 50 authorities. This is not to say that all cyber operations must be covert, but USCYBERCOM is authorized to conduct such operations.

Some believe that USCYBERCOM is an atypical organization that brings strength to the cyber world by the unique status of its commander and his double role as director of the National Security Agency (NSA). This strength comes in part from the juxtaposition of the Title 10 Traditional Military Activities (TMA) authorities of USCYBERCOM and the Title 50 intelligence collection authorities of the NSA. Having NSA and USCYBERCOM in the same location, with the same commander, provides the military with unique capabilities of both commands, and improves Title 10 in Title 50 support to the geographical combatant commanders.[100]

In his article "Demystifying the Title 10-Title 50 Debate," Andru Wall notes "Title 10 is used colloquially to refer to DOD and military operations, while Title 50 refers to intelligence agencies, intelligence activities, and covert action."[101] Although Title 50 is generally associated with the intelligence agencies, it is worth noting that the

[100] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 3, no. 1 (2011): 90–120.

[101] Ibid., 87.

Secretary of Defense maintains substantial powers within Title 50. Wall goes on to paraphrases Richard Gross, author of *Different Worlds: Unacknowledged Special Operations and Covert Action* by stating, “unacknowledged unconventional or cyber warfare may legally be conducted when directed by the President and Secretary of Defense in preparation for an anticipated conventional conflict, and those unacknowledged activities are excluded from the definition of covert action.”[102]

The Title 10 / Tile 50 debate is an often cited as a reason why the military or USSOCOM for that matter should not conduct cyber operations, as the TMA clause in Title 10 does not authorize the conduct of covert operations, which falls under Title 50. However, the TMA clause does allow the military to conduct unacknowledged activities. These cyber operations are not classified ar4 covert action because they are bundled under the TMA clause.”[103]

Although the TMA and Title 50 authorities nested under the SecDef look as if they afford the same value as the USCYBERCOM/NSA relationship, the proverbial intelligence/DOD community ‘rice bowls’ will continue to be guarded. Therefore, for the sake of time and bureaucracy, the dual-hatted nature of the USCYBERCOM commander will most likely be the preferred bridge between the two communities.

9. Cost and Budget

The final criterion is cost and budget constraints. As the nation prepares to downsize the military, the DOD must remain good stewards of governmental funds and not incur unnecessary costs. Unnecessary costs described in the research are defined as the building of new cyber forces and/or procuring unbudgeted cyber equipment.

In contrast to other domains of warfare producing a strategic effect in the cyber domain does not require a large convoluted budget, thousands of warfighters, tracts of land, or hefty gear reserves. Low investments and entrance into networks that are

[102] Ibid., 140.

[103] Andru E. Wall, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action,” *Harvard National Security Journal* 3, no. 1 (2011). 122.

available to the majority of the world's population can offer entry into an adversary's network. Unfortunately, as it stands, contrary to USSOCOM, USCYBERCOM as of 2016 does not yet have its own budget to man, equip or train its own cyber forces and must ultimately rely on the services to fill this roll. If USCYBERCOM is elevated to a unified command status, this will no longer be an issue, but as is, USCYBERCOM is at a huge disadvantage. Therefore, even though the world of cyber warfare is cheap and easily accessed, the hierarchal nature of the Defense Department budgetary may prevent USCYBERCOM from quickly reacting to today's modern battlefield.

With the criterion in mind, the creation of new cyber forces or procurement of new cyber technologies may not be as difficult as they seem. Furthermore, it is also possible to assume the budgetary process for USCYBERCOM today may not model what the process will be in the future. President Elect Trump has identified cyber operations as one of his top five priorities. With this increased focus, it possible that certain budgetary procedures, specific to USCYBERCOM, could be streamlined for efficiency.

D. CONCLUSION

This chapter identified and analyzed nine criteria for assessing whether USCYBERCOM's support to USSOCOM is sufficient or if USSOCOM should establish an internal cyber element. Each criterion identified a series of positives and negatives that both support and refute the current USCYBERCOM support model. Although the results do not show one approach as being clearly superior to the other, their relative merits may become more apparent as USSOCOM gains experience in the cyber domain and USCYBERCOM matures.

For this reason, the researcher recommends that USSOCOM continue to evaluate the current operational support structure provided by USCYBERCOM while further investigating options for future cyber-SOF development. To that end, the following chapter uses decision theory to evaluate different approaches for building a cyber element within USSOCOM. The decision theory analysis did not include the top-level question of whether USSOCOM's cyber requirements is best met by USCYBERCOM or by a SOF-specific internal force, as that question was better addressed through the analysis of this chapter, which draws on different criteria.

With regard to USCYBERCOM's current operations, the researcher recommends they address two critical shortcomings. The first is language and cultural training. Similar to the Special Forces training pipeline, future cyber operators are prepared to support the COCOMs if they received theater specific training. Therefore, USCYBERCOM should, at a minimum, implement a language and region/theater specific coding program to address cultural nuances in cyber domain.

The second shortcoming is the procurement timeline. The MFP-3 procurement process takes too long and does not allow USCYBERCOM the ability to react quickly. If USCYBERCOM were to adopt USSOCOM's procurement rapid acquisitions model, the command may increase its efficacy in support of the COCOMs.

IV. BUILDING USSOCOM'S CYBER CAPABILITY

This chapter utilizes operational design and decision theory to analyze the potential creation of a SOF cyber capacity. The purpose of utilizing decision theory and operational design is twofold. For the military audience, operational design, as part of operational art, is the definitive military process for analyzing a problem set which ultimately allows the commander to make an informed decision. In contrast, decision theory is used more in the academic world. Decision theory gives a decision maker the opportunity to objectively analyze the information at hand and make a decision that is impartial to commander influence.

A. DEFINING OPERATIONAL DESIGN

The military's process of operational design, though still evolving, is an iterative approach to defining an existing or forthcoming problem and then developing an initial strategy or plan to approach that problem. By understanding the task or problem, planners can shape the most appropriate output for the customer, or in the case of USSOCOM, the GCCs. A fundamental component of the operational design process is that the military planner must accurately and unmistakably understand the problem. The planner must comprehend how that problem presents an opportunity to the organization, and then provide the commander with all essential information so the best-informed decision can be made.

Operational design requires an understanding of what capabilities an organization needs to achieve the end-state of the overall strategic plan. Operational design is fundamentally an examination of the ends, ways, means, and risk to overcome a problem. To be successful, operational design requires early identification of the problem's center of gravity or multiple centers of gravity in the case of cyber and the different actors and operational environments involved. All of these elements come together in a comprehensive strategy, allowing the commander an opportunity to understand and grasp the gravity of the mission fully. The culmination of operational design leads the staff and the commander into the Joint Operating Planning Process (JOPP), the next phase of operational art.

When a military component undertakes operational design, it is critical to understand where the unit is in time and space, what the problem is, and where the unit wants to go. The time/space analysis is critical, as an organization cannot arrive at its desired destination if it is oblivious to its current whereabouts. The military component must analyze the external environment as well as the internal. The analysis should result in a thorough and well-defined problem statement that holistically identifies the problem. Finally, a unit requires a well-defined objective to properly address the unit's (destination) end-state. Analyzing the three critical factors of where the unit is in time and space, what the problem is, and what the end state is, provides a foundation for formulating a plan to address the problem. Whether planning is facilitated through JOPPs (Joint Operational Planning Process) or further analysis of the problem statement warranted, there is little doubt that operational design plays a critical role in addressing a problem.

With the operational design framework in mind, Chapter II described the operational environment and how cyber operations could be applied. The chapter provided the reader a snapshot of how USSOCOM could best implement cyber operations in accordance with 12 Core Activities. Chapter III furthered the time space analysis by assessing whether the cyber support provided by USCYBERCOM is adequate to meet USSOCOM's operational requirement or if USSOCOM would be better served by having its own internal cyber capacity to meet its operational requirements. Because that analysis was inconclusive, the researcher recommends investigating how USSOCOM could build a cyber element while evaluating the current cyber-support structure through USCYBERCOM. The remainder of this chapter examines how USSOCOM could create its own cyber forces.

B. DESIRED END STATE

The end-state for USSOCOM would be a fully operational, subordinate, cyber component command in direct support of USSOCOM. This is not to say USCYBERCOM will go away, but some cyber support to SOF will be organic to USSOCOM. This opportunity allows USSOCOM to ripen cyber warfighting as an essential segment of combatant command operations. Launching an intra-SOF cyber organization would consolidate cyber planning and execution within USSOCOM and give the SOF component commands a focal point to synchronize cyber activities.

A potential organizational structure for USSOCOM that would incorporate the proposed cyber component command is shown in Figure 5. The cyber special operations command could function in an analogous fashion to the pre-established component commands under USSOCOM.

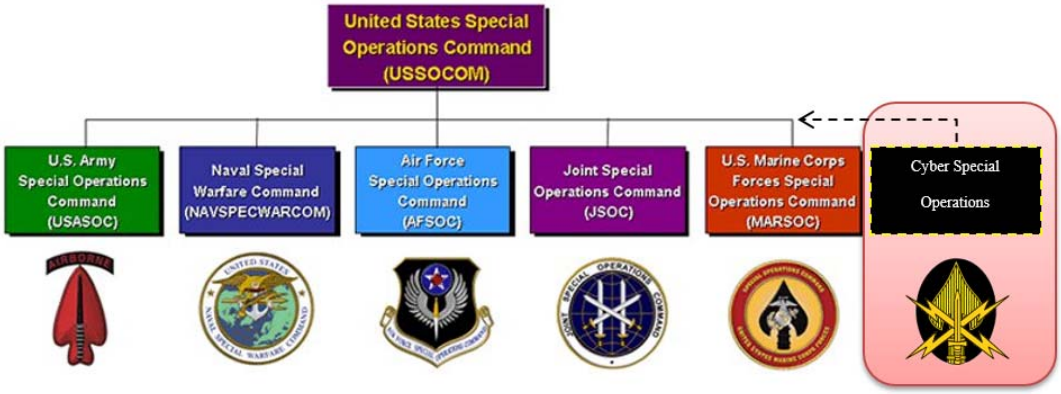

United States Special Operations Command (USSOCOM)
U.S. Army Special Operations Command (USASOC)
Naval Special Warfare Command (NAVSPECWARCOM)
Air Force Special Operations Command (AFSOC)
Joint Special Operations Command (JSOC)
U.S. Marine Corps Forces Special Operations Command (MARSOC)
Cyber Special Operations
AIRBORNE

Figure 5. Potential Cyber Component Command

The unit would most probably entail a commander in the rank of a general officer and a full staff to accomplish its mission of cyber special operations training, manning, equipping, and supporting cyber operational requirements from the TSOCs. The organization could assume responsibility for supporting all SOF cyber operations, including cyber defense, offense, and exploitation. SOF TSOCs might submit yearly cyber requirements to USSOCOM. Then, based on mission priorities, USSOCOM could direct the SOF Cyber Commander to support the TSOCs as required, allowing the USSOCOM Commander to achieve the best organizational fit to support the GGCs.

For the purpose of brevity, the cyber component command will be referred to the Joint Cyber Special Operations Command (JCSOC). Similar to the component commands currently nested within USSOCOM, the JCSOC can serve as a cyber support component for the Special Warfare and Surgical Strike missions. The unit would be fundamentally tasked with supporting USSOCOM’s core activities and providing cyber combat development and subject matter expertise to the headquarters.

The JCSOC, as portrayed in Figure 6, could be divided along three central lines of effort. The first line, defined in name only as the Integration Branch, could liaise with interagency and civilian stakeholders to certify the organization is able to harmonize cyber operations within the whole of government approach. The second line of operation, Support to USSOCOM Headquarters, could deliver internal cyber protection to USSOCOM’s network and conduct cyber capability development in support of special operations. The third line of operation, the Deployable or Operational Component, could support the tactical employment of cyber operations in support of Surgical Strike and Special Warfare missions.

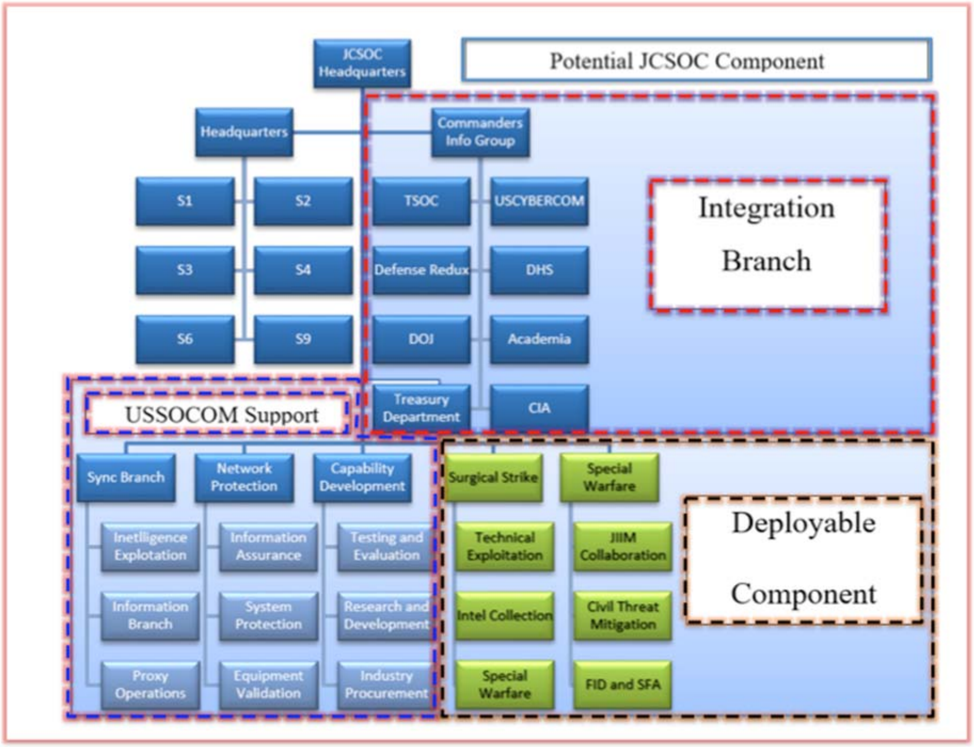


Figure 6. Proposed Organization Structure

C. DECISION THEORY ANALYSIS

Decision theory is a mathematical approach for evaluating choices against different risks and goals. These choices can be represented as branches in a tree that illuminate different paths or courses of action that lead to different outcomes. Decision theory is a common methodology used both in industry and military organizations. It allows an organization the opportunity to visually map a decision and its subsequent sequels.

As noted earlier, the research applied decision theory to the question of "how" to build a cyber capability in USSOCOM rather than "if" the capability should be pursued. The higher-level question was not included in the decision theory analysis as it employed different criteria that were best analyzed separately and not included in a decision tree.

A decision tree for analyzing different paths to developing a JCSOC with USSOCOM is shown in Figure 7.[104] The boxes, labeled A through O, denote the 15 junctures or decision points, while the lines, numbered 1 through 30, denote the branches. The colors of the boxes distinguish the junctures at different levels in the tree. The colors of the branches distinguish the preferred choices (green) from the less desirable ones (red). The decision criteria for evaluating each choice are based on four critical factors: USSOCOM commander acceptability, impact to core activities, funding/resources available, and time. For each of these four criteria, the two branches associated with a juncture are analyzed to determine which branch is preferred as shown in Figure 8. The preferred branch for the juncture as a whole is then taken to be the one that is preferred the most.

[104] Note: The author decided to utilize use a decision tree to analyze the development of a cyber component command in lieu of whether to build the command because he believed it was more important to show how the component command would be built rather than arguing its existence. The rational for the command was explained in chapter III.

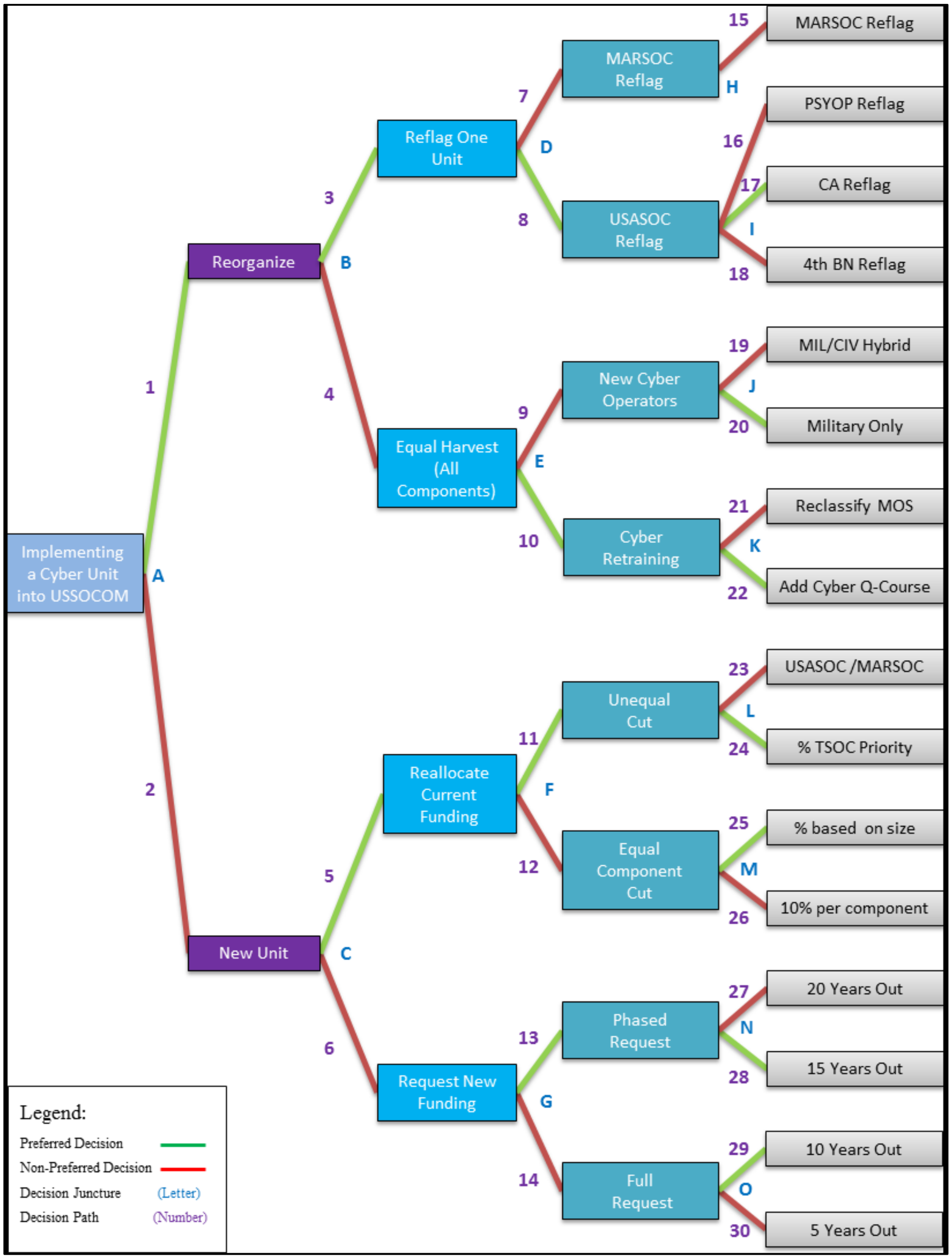
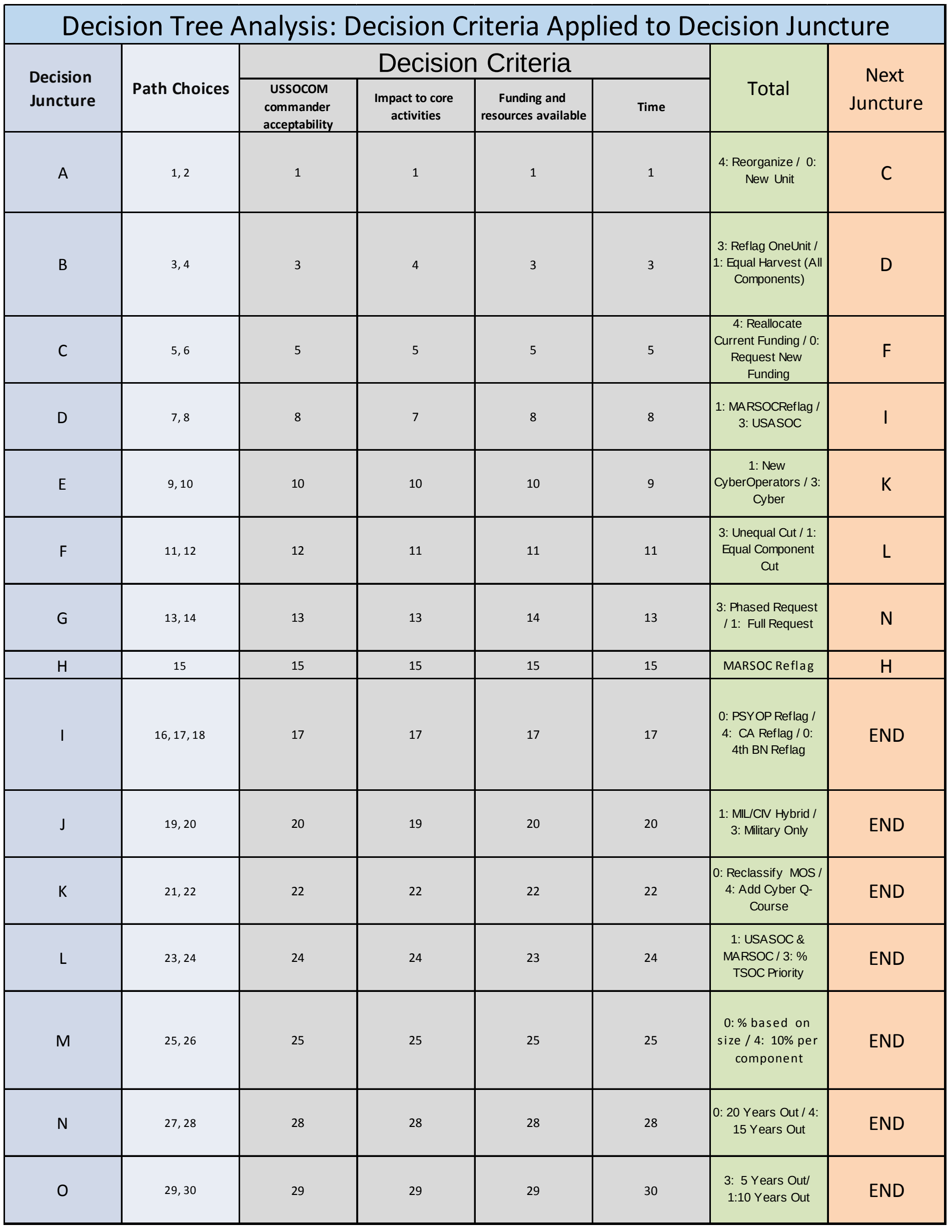


Figure 7. Possible Course of Action



Decision Tree Analysis: Decision Criteria Applied to Decision Juncture

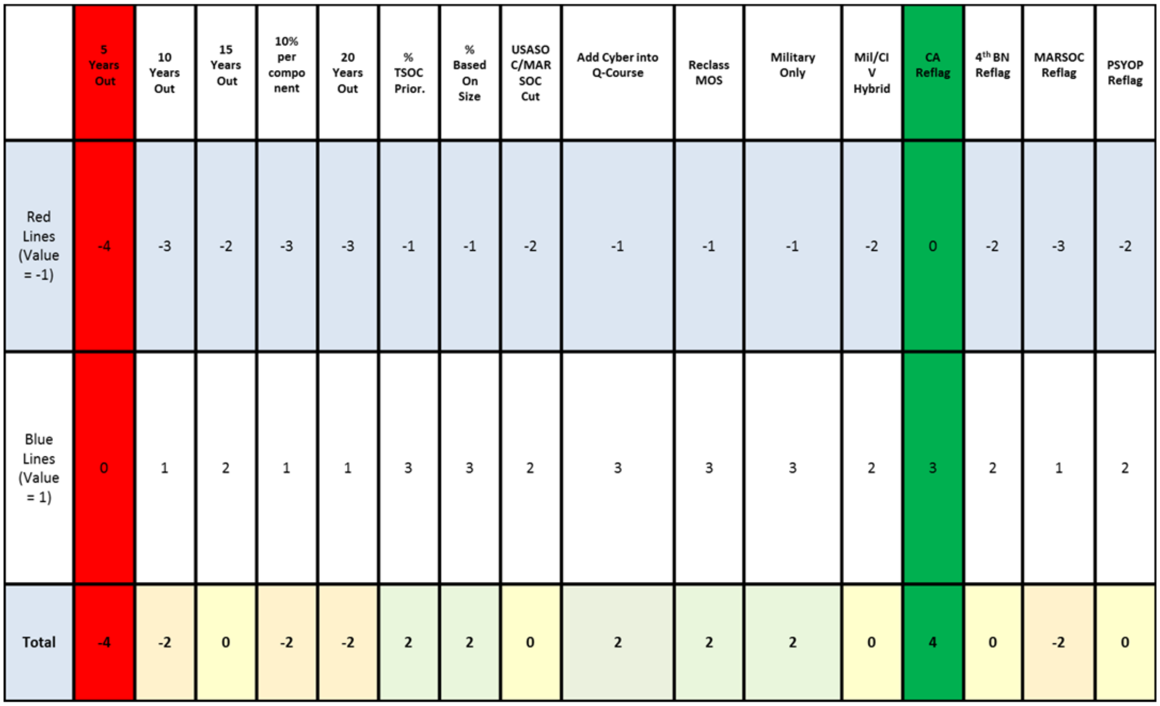
Decision Juncture	Path Choices	Decision Criteria				Total	Next Juncture
		USSOCOM commander acceptability	Impact to core activities	Funding and resources available	Time		
A	1, 2	1	1	1	1	4: Reorganize / 0: New Unit	C
B	3, 4	3	4	3	3	3: Reflag OneUnit / 1: Equal Harvest (All Components)	D
C	5, 6	5	5	5	5	4: Reallocate Current Funding / 0: Request New Funding	F
D	7, 8	8	7	8	8	1: MARSOCReflag / 3: USASOC	I
E	9, 10	10	10	10	9	1: New CyberOperators / 3: Cyber	K
F	11, 12	12	11	11	11	3: Unequal Cut / 1: Equal Component Cut	L
G	13, 14	13	13	14	13	3: Phased Request / 1: Full Request	N
H	15	15	15	15	15	MARSOC Reflag	H
I	16, 17, 18	17	17	17	17	0: PSYOP Reflag / 4: CA Reflag / 0: 4th BN Reflag	END
J	19, 20	20	19	20	20	1: MIL/CIV Hybrid / 3: Military Only	END
K	21, 22	22	22	22	22	0: Reclassify MOS / 4: Add Cyber Q-Course	END
L	23, 24	24	24	23	24	1: USASOC & MARSOC / 3: % TSOC Priority	END
M	25, 26	25	25	25	25	0: % based on size / 4: 10% per component	END
N	27, 28	28	28	28	28	0: 20 Years Out / 4: 15 Years Out	END
O	29, 30	29	29	29	30	3: 5 Years Out/ 1:10 Years Out	END

Figure 8. Decision Tree Analysis: Decision Criteria vs. Decision Juncture

The numbers shown in Figure 9 quantifiably represent the decisions made in the decision tree. Each preferred decision (green line) is assigned a value of +1, while each un-preferred decisions (red line) is assigned a value of -1. The values of +1 or -1 were determined as an aggregate of Row 8 in Figure 8. This rating scheme provides a means of quantifying the total value of each decision. The far left column sums the total number of un-preferred decisions and preferred decisions for each end state, as indicated on the top row. The bottom row indicates the score for each end state, summing the second and third row's values. This score is the sum of the non-preferred and preferred decisions along each path. For instance, the 5-year plan contains four non-preferred decisions and no preferred decisions, therefore receiving a score of -4. The ten year out scenario contains three non-preferred and one preferred, getting a score of a -2.

The easiest course of action, highlighted in dark green, is to reorganize the 95th Civil Affairs Brigade, as the United States Army Civil Affairs and Psychological Operations Command (USACAPOC) or 1st Special Forces Command can easily fill the 95ths current CAO mission. Additionally, Civil Affairs do not have any unique or critical skills specific to the branch. Though the author is a Civil Affairs Officer and understands the decision will most definitely cause heartache and concern, the unit's tasks are easy to replicate. The author also assesses it may also be possible with the high level of Soldier competency in the 95th for CA Soldiers to retrain and fulfill the cyber requirement. With the reorganization of the 95th, nearly 2000 billets will become available for re-designation—more than enough to meet the minimal 100-team SOF cyber operating requirements.

Choosing to develop a new unit in five years, as highlighted in dark red (Column '5 years out'), is the most difficult and the most resource intensive. It would be nearly impossible for the command to resubmit the Program Objective Memorandum (POM) with the changes required to fill such a huge organizational change. To submit and fund the request, the process would most definitely require the Joint Chief of Staff's approval and strict oversight. Otherwise, this course of action is impractical.



	5 Years Out	10 Years Out	15 Years Out	10% per component	20 Years Out	% TSOC Prior.	% Based On Size	USASOC/MARSOC Cut	Add Cyber into Q-Course	Reclass MOS	Military Only	Mil/CIV Hybrid	CA Reflag	4th BN Reflag	MARSOC Reflag	PSYOP Reflag
Red Lines (Value = -1)	-4	-3	-2	-3	-3	-1	-1	-2	-1	-1	-1	-2	0	-2	-3	-2
Blue Lines (Value = 1)	0	1	2	1	1	3	3	2	3	3	3	2	3	2	1	2
Total	**-4**	**-2**	**0**	**-2**	**-2**	**2**	**2**	**0**	**2**	**2**	**2**	**0**	**4**	**0**	**-2**	**0**

Figure 9. Decision Tree Scoring (Preferred vs. Non-Preferred Decisions)

1. Preferred Decision

The first Juncture (A) in the tree requires that USSOCOM decide whether to build a new component command or reorganize under the current organizational structure. Keeping in mind the pre-established decision criteria (Commander Acceptability and Impact to Core Activities), the command best accepts this decision because they believe in the concept of better, not bigger.[105] This decision is also supported because of the current DOD imposed fiscal restraints and future budget uncertainty. Finally, with the ever-progressing domain of cyber warfare, reorganizing would be the quickest method to building a SOF cyber capacity. Thus, branch 1 from juncture 8 is preferred according to all four criteria, as shown in Figure 8. The preferred course of action for this decision is to reorganize.

[105] Ferdinando, Lisa, "Army Special Operations Command Evolves in Changing World," Www.army.mil. January 27, 2015. Accessed September 13, 2016. https://www.army.mil/article/141746/Army_Special_Operations_Command_evolves_in_changing_world.

Assuming a decision to reorganize, the next decision Juncture (B) would be to determine whether this were best done by reassigning an equal portion of billets from each SOF component command to the new unit (branch 4) or designating one component to reorganize (branch 3). For this decision, the researcher believes USSOCOM would designate one unit to reorganize. The researcher believes that because of SOF component command budgets, it would be easier for one component to bear the entire responsibility. Additionally, some commands are much larger than others and have different demand signals. Requiring all commands to give up billets may not be the most conducive methodology for USSOCOM. However, it should be noted that branch 3, while preferred for three of the four criteria, was not preferred in terms of impact on core activities.

Assuming USSOCOM chooses to reorganize an existing component, the next Juncture (D) requires selecting the component for reorganization. NAVSPECWARCOM (Naval Special Warfare Command) and AFSOC (Airforce Special Operations Command) were omitted from this decision because they both offer unique capabilities that could not be replicated in MARSOC (Marine Special Operations Command) or USASOC. Therefore, left with the decision between USASOC (branch 8) and MARSOC (branch 7), the command should choose USASOC. USASOC currently has the most billets of any special operations component command and its capabilities could be replicated in other commands or internally among its forces. MARSOC, in contrast, is too thin for reorganization and does not have the manpower or the experience at the staff level to handle such a large change.

The final Juncture (I) along the reorganization path involves determining which unit within USASOC to reorganize. The decision is left between the 95th Civil Affairs Brigade, 8th Military Information Support Group or PSYOP (branch 17), or the fourth Battalions from each Special Forces Group (branch 18). The reason for considering only the fourth Battalions is that they have the most controversial and publicly contested mission (UW) in USASOC. Reflagging them would be politically palatable in congress. However, the researcher believes it is USSOCOM's best interest to reorganize the 95h Civil Affairs Brigade's billets. 95th is the only unit in USASOC that does not possess any technical or non-replicable skills. In fact, prior to the establishment of an official civil affairs MOS (military occupational specialty), Civil Affairs Operations were conducted by Special Forces soldiers. This transition would also be the most cost-effective, as the 95th does not have a large stockpile of mission specific equipment. The researcher estimates with the closure of the 95th, USASOC could reorganize rather efficiently to ensure the Special Forces Groups quickly assumed all CAO missions.

2. Alternate Decisions

The second-best decision is difficult to quantify because five alternate decision paths quantifiably fall in second place (Score 2). Two of these resulted from choosing to build a new unit, while three of the five resulted from reorganizing. Additionally, it is difficult to compare and contrast because junctures between sequels are not comparable. As an example, Juncture B - reflag one unit and equal harvest, cannot compare to Juncture C—reallocate current funding and request a new unit, because they are incomparable. At end state, the researcher cannot definitely say which course of action is second or third best, but the researcher does provide a potential outlook on what other courses of action may entail as weighted against the decision criteria.

The first alternate decision is to build a new SOF cyber component command by reallocating current SOF funding and taking an unequal cut from each existing SOF component command based on TSOC mission requirements. This decision is one of the five-second best decisions and scored overall 3 positive decisions and 1 negative. With the exception of the first negative decision at Juncture A; Junctures C, F, and L were positive decision paths. In light of the reasoning for Juncture A, above in the section labeled Primary Decision, the researcher will address the rationale for the decisions made at Juncture's C, F, and L.

Juncture C determined that based on the four decision criteria, reallocating current funding for a new cyber unit would be the best decision. The USSOCOM commander would most likely accept this course of action because as stated earlier in the research, "new money" is a politically unpopular topic within the DOD but once the current budget is appropriated, the command can then re-appropriate the funds as necessary. Concerning impact to core activities and time, if the command were to reallocate current funding, there may be a 5-year funding cycle negative impact to USSOCOM's ability to conduct its traditional assigned responsibilities.

Following Juncture C is Juncture F. At Juncture F, USSOCOM would need to decide when building the new cyber component command if it will require all components to reduce its budgets or enforce an unequal cut across the command. For this decision, the researcher believes USSOCOM would enforce an unequal cut based on the application of the decision criteria. From a commander's perspective, it would be easier for General Thomas to direct all four subordinate component commands to reduce their budget rather than "going into the weeds" with one. Conversely, if USSOCOM were to direct an unequal cut, USSOCOM could preserve its ability to support its most critical core activities while marginalizing those that are not as important. An unequal cut also makes the most sense from a budgetary standpoint as not all SOF component commands have the same budget. USASOC tends to receive more budgetary support from the Department of the Army in comparison to MARSOC and the Department of Navy. Finally, concerning time, directing an equal cut among all components would take months if not years of negotiations with the SOF components and therefore not be conducive.

D. CONCLUSION

This thesis examined the supporting cyber relationship between USSOCOM and USCYBERCOM. It also analyzed USSOCOM's two main missions, Special Warfare and Surgical Strike, in order to determine how cyber operations could support each mission and their core activities. By analyzing USCYBERCOM and its cyber support to USSOCOM, the thesis was able to address the main research question and two subordinate questions.

The main question asks: is USSOCOM's posture for cyber operations sufficient for the current and future operating environment? This research found it to be lacking for both the current and future operating environment. USSOCOM requires further cyber capabilities as provided in the form of either an internal or external cyber organization (USCYBERCOM). The research is inconclusive as to which course of action is best, internal or external, but does provide a potential course of action if USSOCOM decides to develop an internal cyber command.

Sub-question, one addresses whether or not the elements of USSOCOM's core activities are sufficient as is or has room for improvement through the incorporation of cyber operations. Through the analysis of USSOCOM's 12 core activities and potential incorporation of cyber warfare, there appears to be much room for improvement. Each of the 12 core activities could be greatly enhanced if cyber techniques, tactics, and procedures were applied.

The final sub-question is whether USCYBERCOM's cyber support arrangement meets USSOCOM's requirement or if USSOCOM needs its own internal cyber force. The results here were inconclusive. If USSOCOM determines at some point the need for an internal cyber command, the researcher recommends that USSOCOM turn to the analysis of Chapter IV. Through the application of decision theory and operational design, the analysis suggests that the unit is best acquired by reorganizing USSOCOM's existing combat components, in particular, by reflagging the 95th Civil Affairs Brigade of USASOC. The reflagging of the 95th seems to offer the best solution in terms of manpower, resources, and mission.

If USSOCOM were to build a cyber unit in support of special operations, it would require in-depth planning and a multi-stakeholder approach. This approach would most likely require input from all levels of government. Interagency and civilian leaders alike must be included to ensure a potential unit considers all angles of cyber warfare.

E. FUTURE WORK

The cyber domain is constantly evolving and presenting new information and challenges every day. This constant change presents unique opportunities to both current and future researchers. Suggestions for future research questions include: 1) How

USCYBERCOM's potential elevation to a unified command will affect USSOCOM's operations. 2) If USSOCOM were to build a cyber component command, what would that command look like? 3) How best can USSOCOM incorporate cyber into its command without producing additional billets? 4) What would be the best mix of civilian and military cyber operators within USSOCOM? 5) What would it take budget-wise to build a component command in USSOCOM? Though the future work research list covers major ideas within the USSOCOM cyber debate, the list is not all-inclusive. If USSOCOM were to build a cyber component command, it would require a major investment from USSOCOM staff and DOD writ large.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Applegate, Scott D. “The Dawn of Kinetic Cyber.” *In Cyber Conflict (CyCon)*, 2013 5th International Conference on, pp. 1–15. IEEE, 2013.

“ARSOF Operating Concept.” Special Operations Command. September 26, 2014. Accessed May 5, 2016. http://www.soc.mil/Assorted Pages/ARSOF Operating Concept 2014.pdf.

Bucci, Steve. “The Importance of Special Operations Forces Today and Going Forward.” The Heritage Foundation. Accessed May 4, 2016. http://index.heritage.org/military/2015/important-essays-analysis/importance-special-operations-forces-today-going-forward/.

Clarke, Richard, and Robert Knake. *Cyber War*. New York, USA: Harper Collins, 2011.Clapper, James R. “Worldwide Threat Assessment to the House Permanent Select Committee on Intelligence.” *Statement for the Record, House Permanent Select Committee on Intelligence, 112th Cong., 2nd Sess* (2012): 1.

“Department of Defense Strategy for Operating in Cyberspace.” National Institute for Standards in Technology. July 2011. Accessed December 15, 2016. csrc.nist.gov/groups/SMA/ispab/.../DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Duggan, Patrick. “Man, Computer, and Special Warfare.” *Small Wars Journal*. January 4, 2016. Accessed December 14, 2016. http://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare.

———. “Strategic Development of Special Warfare in Cyberspace.” *Joint Force Quarterly 79, 4th Quarter* (December 2015): 46-53, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_46-53_Duggan.pdf.

———. “Why Special Operations Forces in U.S. Cyber-Warfare?” The Cyber Defense Review. January 8, 2016. http://www.cyberdefensereview.org/2016/01/08/why-special-operations-forces-in-us-cyber-warfare/.

Feickert, Andrew. *U.S. Special Operations Forces (SOF): Background and Issues for Congress* (CRS Report No. RS21048). Washington, DC: Congressional Research Service, 2016. https://fas.org/sgp/crs/natsec/RS21048.pdf

Ferdinando, Lisa. “Army Special Operations Command Evolves in Changing World.” AR News. January 27, 2015. Accessed September 13, 2016. https://www.army.mil/article/141746/Army_Special_Operations_Command_evolves_in_changing_world.

Fitzgerald, Ben, and Parker Wright. “Digital Theaters: Decentralizing Cyber Command and Control.” Disruptive Defense Papers: Center for a New American Security. April 24, 2014. Accessed December 14, 2016. https://www.cnas.org/publications/reports/digital-theaters-decentralizing-cyber-command-and-control.

Forbes, Philip M. “Son of SPECOPS: Rethinking the Nature and Operationalization of Cyberspace”. Final Paper, Naval War College Newport Rhode Island Joint Military Operations Department, 2012.U.S. Joint Chiefs of Staff. *Special Operations*.

Joint Publication 3-05. Washington, DC: Joint Chiefs of Staff, April 18, 2010.U.S. Joint Chiefs of Staff. *Special Operations*.

Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.

Lucas, Edward. *Cyberphobia: Identity, Trust, Security and the Internet*. (London: Bloomsbury Publishing USA, 2015). http://www.bloomsbury.com/uk/cyberphobia-9781408850138/.

Magnuson, Stew. “Do Cyberwarriors Belong at Special Operations Command?” *National Defense Magazine*. August 01, 2011. http://www.nationaldefensemagazine.org/archive/2011/August/Pages/DoCyberwarriorsBelongatSpecialOperationsCommand.aspxMarkoff,

Markoff, John, and David Sanger. “In a Computer Worm, a Possible Biblical Clue.” *The New York Times*. September 29, 2014. http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html.

Maxwell, David S. “Thoughts on the Future of Special Operations” Small Wars Journal. October 31, 2013. http://smallwarsjournal.com/jrnl/art/thoughts-on-the-future-of-special-operations

Mulford, Laurie A. “Let Slip the Dogs of (CYBER) War: Progressing Towards a Warfighting U.S. Cyber Command.” National Defense University Norfolk VA Joint Advanced Warfighting School, 2013.

Nakishima, Ellen. “Pentagon Cyber Unit Wants to ‘Get Inside the Bad Guy’s Head’.” *The Washington Post*, June 19, 2014. https://www.washingtonpost.com/news/checkpoint/wp/2014/06/19/pentagon-cyber-unit-wants-to-get-inside-the-bad-guys-

Pomerleau, Mark. “Cyber Command Getting Closer to Full Deployment -- Defense Systems.” Defense Systems. June 23, 2016. https://defensesystems.com/articles/2016/06/23/cyber-command-gets-closer-to-full-deployment.aspx.

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Georgetown University Press, 2012, 155

Rosenzwelg, Paul. “The New Face of Law and Cyber Warfare.” LawFare. October 18, 2016. https://www.lawfareblog.com/new-face-law-and-cyber-warfare.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* New York: PublicAffairs, 2016, 2.Tanner, Leah. “Examining Cyber Command Structures.” Master’s thesis, Naval Postgraduate School, 2015.

U.S. Joint Chiefs of Staff. *Foreign Internal Defense*. Joint Publication 3-22. Washington, DC: Joint Chiefs of Staff, July 12, 2010.

U.S. Cyber Command. Beyond the Build, Delivering Outcomes Through Cyberspace. Washington, DC: Department of Defense, June 3, 2015.

U.S. Strategic Command. “U.S. Cyber Command.” September 30, 2016.http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/

Wall, Andru E. “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action.” *Harvard National Security Journal* 3, no. 1 (December 2011): 90-120. http://harvardnsj.org/2011/12/demystifying-the-title-10-title-50-debate-distinguishing-military-operations-intelligence-activities-covert-action/.

Yarger, Harry R. Building Partner Capacity. McDill AFB, Florida: The JSOU Press, 2015. www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA619818..

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California